MEMORIE VAN TOELICHTING

Inhoudsopgave

Bijlage 1: Transponeringstabel

Bijlage 2: Opbouw wetsvoorstel

Bijlage 3: Overzicht bijzondere bevoegdheden en waarborgen

Bijlage 4: Schematische weergave onderzoeksopdrachtgerichte interceptie

Bijlage 5: Schematisch overzicht wetgeving van enkele andere landen

I. Algemeen deel

Hoofdstuk 1 Inleiding

Met dit wetsvoorstel beoogt de regering de Wet op de inlichtingen- en veiligheidsdiensten 2002 (Wiv 2002) te vervangen. De bestaande wet was toe aan een grondige herziening. Een belangrijke wijziging is dat de bevoegdheden van de inlichtingen- en veiligheidsdiensten worden gemoderniseerd en dat er wettelijke waarborgen voor inzet van die bevoegdheden nauwgezet worden vastgelegd. De memorie van toelichting gaat, zoals gebruikelijk, in op alle aspecten van het wetsvoorstel en op de veranderingen ten opzichte van de Wiv 2002. Gezien de onderwerpen waar dit wetsvoorstel over gaat, is het van groot belang dat nauwgezet en uitvoerig te doen.

In deze inleiding wordt in paragraaf 1.1 allereerst kort het waarom van dit wetsvoorstel geschetst. In paragraaf 1.2 wordt nader ingegaan op de balans tussen modernisering van bevoegdheden en grondrechtelijke waarborgen. Hierover is tijdens de totstandkoming van dit wetsvoorstel veel discussie geweest. Vervolgens komen de achtergronden voor de nagestreefde modernisering van de bevoegdheden van de inlichtingen- en veiligheidsdiensten uitgebreider aan bod in de paragrafen 1.3. en 1.4. De paragrafen 1.5, 1.6 en 1.7 geven een korte toelichting op de totstandkoming van de wet en op de belangrijkste wijzigingen. Het hoofdstuk sluit af met een leeswijzer bij het wetsvoorstel.

1.1. Waarom een nieuwe wet?

Een belangrijke kerntaak van de overheid is het garanderen van een veilig land waarin in vrijheid kan worden geleefd en de democratische rechtsorde is gewaarborgd. Om onze veiligheid te beschermen is een continue inzet nodig van die overheid. In eigen land, in Europa, maar ook ver over de grenzen. Het werk van de inlichtingen- en veiligheidsdiensten is onmisbaar voor onze nationale en internationale veiligheid, gelet op onder meer de toenemende terroristische dreiging, cyberdreigingen, de vele brandhaarden in de wereld en destabilisatie aan de grenzen van Europa.

Er is een inherente spanning tussen enerzijds de democratische rechtsstaat en de daaraan ten grondslag liggende waarden en anderzijds het bestaan en functioneren van inlichtingen- en veiligheidsdiensten. Effectief functionerende inlichtingen- en veiligheidsdiensten maken door gebruik te maken van hun ingrijpende bevoegdheden namelijk per definitie inbreuk op grondrechten, waaronder de privacy. Tegelijkertijd

moeten de diensten in het belang van de nationale veiligheid en de ondersteuning van de krijgsmacht ook in het digitale tijdperk hun taken doeltreffend en doelmatig kunnen blijven uitvoeren, binnen de grenzen van de wet en met eerbiediging van de persoonlijke levenssfeer van burgers. Technologische en maatschappelijke ontwikkelingen, zoals de snelle opkomst en mondiale verspreiding van digitale technologie en het internet, hebben vergaande gevolgen. Deze ontwikkelingen en het genoemde dreigingsbeeld nopen tot modernisering van de bevoegdheden van de inlichtingen- en veiligheidsdiensten.

Wij zijn ons bewust van de genoemde spanning. De afgelopen jaren is het debat hierover in binnen- en buitenland met grote intensiteit gevoerd. Met dit wetsvoorstel willen we die modernisering mogelijk maken. Dit leidt dan wel tot de vraag hoe de balans moet worden gevonden tussen de nieuwe en bestaande bevoegdheden van de inlichtingen- en veiligheidsdiensten (i.c. AIVD en MIVD) aan de ene kant en de grondrechtelijke waarborgen bij de uitoefening daarvan aan de andere kant. Voor ons is het evident dat de beoogde modernisering van de bevoegdheden van de AIVD en de MIVD gepaard moet gaan met een versterking van deze grondrechtelijke waarborgen. Op die manier wordt voorkomen dat de balans te zeer doorslaat naar de zorg voor de nationale veiligheid. De urgentie van dat laatste blijkt ook uit enkele rechterlijke uitspraken.[1] Dit wetsvoorstel versterkt de waarborgen en het toezicht daarom ook aanzienlijk.

1.2. De balans modernisering bevoegdheden-grondrechtelijke waarborgen

Navolgend wordt de in dit wetsvoorstel opgenomen versterking van de waarborgen en het toezicht uiteengezet.

1.2.1. Aangescherpte controle

[1] In dit verband is met name de uitspraak van 22 november 2013 van het Europese Hof voor de Rechten van de Mens (EHRM) van belang in een door "De Telegraaf" c.s. tegen de Staat der Nederlanden aanhangig gemaakte zaak. Het EHRM kwam daarin unaniem tot het oordeel dat de inzet van bijzondere bevoegdheden van de AIVD jegens journalisten van "De Telegraaf" en schending opleverde van de artikelen 8 en 13 van het Europees Verdrag tot bescherming van de Rechten van de Mens en de fundamentele vrijheden (EVRM)(EHRM 22 november 2012, nr. 39315/06). Bij brief van 7 december 2012 heeft de Minister van Binnenlandse zaken en Koninkrijksrelaties, mede namens de Minister van Veiligheid en Justitie, de Tweede Kamer geïnformeerd over de gevolgen die aan deze uitspraak moesten worden verbonden. In vervolg op deze brief is een wetsvoorstel in verband met de invoering van een onafhankelijke bindende toets voorafgaande aan de inzet van bijzondere bevoegdheden jegens journalisten, welke gericht is op het achterhalen van hun bronnen ingediend. Dat wetsvoorstel – inmiddels aanhangig bij de Tweede Kamer – is vervolgens in het voorliggende wetsvoorstel is geïncorporeerd. Zie hiervoor verder in het bijzonder paragraaf 3.3.2.5.2 van deze memorie van toelichting. Andere relevante rechterlijk uitspraken zijn Andere relevante rechterlijke uitspraken zijn: op nationaal niveau de zaak inzake het aftappen van advocaten (Rb Den Haag, 1 juli (KG) ELI:GHDH:7436) en in hoger beroep bevestigd door het Gerechtshof van Den Haag op 27 oktober 2015, ECLI:NL:GHDHA:2015:2881) en een hele reeks EHRM-zaken: Dumitru Popescu tegen Roemenië (EHRM 26 april 2007, nr. 71525/01), Segerstadt-Wiberg e.a. tegen Zweden (EHRM 6 juni 2006, nr. 62332/00), Copland tegen het Verenigd Koninkrijk (EHRM 3 april 2007, nr. 62617/00), Iordachi tegen Moldavië (EHRM 10 februari 2009, nr. 25198/02), Kennedy tegen het Verenigd Koninkrijk (EHRM 2 september, nr. 26839/05), Zakharov tegen Rusland (EHRM 4 december 2015, nr. 47143/06) en Szabo en Vissy tegen Hongarije (EHRM 12 september 2016, nr. 37138/14).

De bevoegdheden van de inlichtingen- en veiligheidsdiensten vragen om aangescherpte controle. De regering realiseert zich dat de bevoegdheden van de diensten verregaand zijn. Het is met vertrouwen dat zij deze geeft aan de AIVD en de MIVD. Meer dan tien jaar toezicht door de CTIVD geeft een beeld van twee inlichtingen- en veiligheidsdiensten die hun taken zorgvuldig uitvoeren, binnen de kaders van de wet. Het vertrouwen van de regering krijgt een stevige basis in versterkte controle. Het controlesysteem is in dit wetsvoorstel aangescherpt. Met een toets voorafgaand aan de daadwerkelijke uitoefening van een bijzondere bevoegdheid door een nieuwe onafhankelijke toetsingscommissie, toezicht tijdens en achteraf van de onafhankelijke CTIVD, en de mogelijkheid een klacht in te dienen bij de CTIVD die in dat geval bindend oordeel geeft, is het stelsel van rechtsbescherming aanmerkelijk verbeterd. Met name het voorafgaand toezicht is fors versterkt. Geheel in lijn met de Europese jurisprudentie op dit terrein kunnen ingrijpende bevoegdheden niet worden uitgeoefend zonder voorafgaande, onafhankelijke toets. Het gehele gebied van toetsing, toezicht en klachtbehandeling wordt daarmee bestreken door commissies die onafhankelijk van elkaar werken.

1.2.2. Transparantie

In dit wetsvoorstel worden de bevoegdheden van de inlichtingen- en veiligheidsdiensten die inbreuk maken op de persoonlijke levenssfeer expliciet beschreven. De regering betracht maximale transparantie over de inzet van de nieuwe bevoegdheid tot onderzoeksopdrachtgerichte interceptie. Natuurlijk kan niet worden geopenbaard tegen wie of voor welk onderzoek de bevoegdheid precies wordt ingezet. Vanzelfsprekend kan de CIVD hierover wel vertrouwelijk worden geïnformeerd en kan de CTIVD op elk gewenst moment onderzoek doen naar de uitvoering van onderzoeksopdrachtgerichte interceptie en hierover in het openbaar rapporteren.

1.2.3. Beperkte schaalgrootte

De rijksoverheid neemt de kosten van de modernisering van de bevoegdheden op zich. Hiermee geeft de regering duidelijk het belang aan van het intercepteerbaar maken van de kabelgebonden infrastructuur. De investeringen die de telecommunicatiesector moet doen, worden naar redelijkheid vergoed. De sector hoeft zich geen zorgen te maken over kosten of concurrentienadeel. Overleg met relevante aanbieders in de telecomsector is voorts nodig 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 sprake van schaalbaarheid in omvang en tijd. De regering beschouwt de in het financiële hoofdstuk genoemde bedragen als kaderstellend

voor de uitoefening van de bevoegdheid (inclusief de vergoeding van de kosten die door het bedrijfsleven worden gemaakt). Daarmee wordt tevens de doelmatige en doeltreffende inzet van de bevoegdheid bevorderd.

1.2.4. Niet-relevante data worden vernietigd

Als data rechtmatig zijn vergaard, betekent dat dan dat deze daarna voor altijd worden bewaard en steeds weer kunnen worden gebruikt? Nee, het eventuele verdere gebruik van data is aan strikte wettelijke regels gebonden. De diensten moeten via bijzondere bevoegdheden verkregen data zo spoedig mogelijk op relevantie onderzoeken. Data die niet relevant zijn, worden verwijderd en vernietigd. Voor onderzoeksopdrachtgerichte interceptie is de maximale bewaartermijn op drie jaar gesteld. Wij sluiten hiermee op hoofdlijnen aan op hetgeen gebruikelijk is in de landen om ons heen. De regering acht het noodzakelijk en legitiem dat deze termijnen bestaan: om dreigingen te kunnen wegnemen is het cruciaal om terug te kunnen kijken in datasets. Dat blijkt uit (internationaal) onderzoek naar aanleiding van de aanslagen in Frankrijk in 2015 en uit vele andere onderzoeken van de AIVD, de MIVD en Europese partnerdiensten in de afgelopen jaren. Hetzelfde geldt voor het onderzoek naar de langlopende, structurele aanvallen op onze ICT-infrastructuur door vijandige, statelijke cyberactoren. De regering wijst er op dat het hierbij om datasets gaat, die reeds relevant zijn bevonden voor de taakuitoefening van de diensten en die vervolgens op basis van nadere toestemming en toetsing worden verwerkt. Er is geen sprake van het bewaren van data van personen en organisaties die niet relevant zijn in het kader van een dreiging.

1.2.5. Internationale samenwerking: vier sloten op de deur

Kunnen de rechtmatig vergaarde gegevens onbeperkt worden uitgewisseld met buitenlandse partners? Deze vraag is in de internetconsultatie veel gesteld. De regering benadrukt dat intensieve internationale samenwerking, en daarmee ook de uitwisseling van ongeëvalueerde gegevens, onmisbaar is. Of het nu gaat om het uitwisselen van *identifiers* van terroristen die Europa inreizen, het uitwisselen van *signatures* van cyberaanvallen gericht op het hoogwaardig Europees bedrijfsleven of het met bondgenoten uitvoeren van militaire operaties in brandhaarden over de wereld: de razendsnelle uitwisseling van gegevens blijft doorslaggevend voor het nemen van adequate tegenmaatregelen. Bijvoorbeeld omdat een jihadist in België of Frankrijk in mum van tijd in Nederland kan zijn. Maar ook omdat pas als de afzonderlijke puzzelstukjes in elkaar vallen, het werkelijke gezicht van de dreiging zich laat zien.

Dit betekent niet dat de regering daarbij als het ware onze achterdeur wagenwijd openzet. Integendeel: voor de internationale uitwisseling van ongeëvalueerde gegevens is er één deur en die is voorzien van vier sloten. Allereerst kan enkel met anderen

worden gedeeld wat rechtmatig door onze diensten is vergaard (eerste slot). Ten tweede werkt Nederland samen met betrouwbare partners, waarbij de uitwisseling van ongeëvalueerde gegevens slechts met een zeer beperkt aantal landen plaatsvindt. Eerbied voor de mensenrechten en democratische inbedding worden gewogen, voordat er wordt samengewerkt. Dat is nu ook opgenomen in het wetsvoorstel zelf (tweede slot). Het derde slot is dat enkel gegevens kunnen worden uitgewisseld nadat de minister hier toestemming voor heeft gegeven. Tot slot, en dat is het vierde slot, houdt de CTIVD toezicht op deze praktijk. Dat heeft zij sinds 2002 ook meermaals gedaan en geconcludeerd dat het verstrekken van verzamelingen gegevens, zowel metagegevens als inhoudelijke communicatie, in de onderzochte samenwerkingsverbanden rechtmatig plaatsvindt.

1.2.6. Taakgebondenheid en proportionaliteit

Zoals ook in de Wiv 2002 reeds het geval is, zijn in het wetsvoorstel de taken van de AIVD en de MIVD gedefinieerd. Buiten deze taken kan niet worden getreden. De taken worden inhoudelijk ingevuld door de Geïntegreerde Aanwijzing, waarin de regering in de richting van de diensten aangeeft wat noodzakelijk wordt geacht voor een veilig Nederland, voor een goed geïnformeerde regering en voor de internationale veiligheid. De onderzoeken van onze diensten zijn dus zeer helder ingekaderd. In de openbare jaarverslagen en de jaarplanbrieven aan de Tweede Kamer is te lezen welke de onderzoeksgebieden van de diensten zijn.

Verder is van belang dat iedere inzet van bevoegdheden door de AIVD of de MIVD moet voldoen aan drie vereisten:

(1) Proportionaliteit. Het doel moet opwegen tegen de inbreuk op de privacy en deze inbreuk rechtvaardigen. Een voorbeeld: een netwerkserver kan worden gehackt om een aanslag te voorkomen, niet om enkel te bezien of vanuit het netwerk soms opruiende boodschappen *online* worden gezet.

(2) Subsidiariteit. Het lichtste middel waarmee het doel kan worden bereikt moet worden gekozen. Een voorbeeld: om uitreisplannen te onderkennen wordt geen onderzoeksopdrachtgerichte interceptie ingezet, als door gesprekken in de directe omgeving hetzelfde resultaat kan worden bereikt.

(3) Doelgerichtheid. Op voorhand moet een specifiek doel worden aangegeven en de uitoefening van de bevoegdheid moet in overeenstemming zijn met dat doel. Een voorbeeld: onderzoeksopdrachtgerichte interceptie vindt niet plaats om alle communicatie in de stad Den Haag een maand lang te verzamelen, om dan te bezien of voor de diensten relevante gegevens zijn binnengehaald.

1.3. Waarom modernisering van bevoegdheden?

1.3.1. Een kerntaak van de overheid

Eén van de kerntaken van de overheid, is het garanderen van een veilig land waarin in vrijheid kan worden geleefd en de democratische rechtsorde is gewaarborgd. Al geruime tijd nemen dreigingen van terrorisme, cyberaanvallen en onrust aan de grenzen van Europa toe. Binnen Europa worden geregeld dodelijke aanslagen gepleegd. Er moet rekening worden gehouden met brandhaarden op verschillende plekken in de wereld die niet zullen doven maar juist zullen opvlammen, met directe gevolgen voor Europa en Nederland. Om onze veiligheid te beschermen is een continue inzet nodig van de overheid. In eigen land, in Europa, maar ook ver over de grenzen. Onder meer met diplomatieke en militaire middelen.

1.3.2. Technologische ontwikkelingen

De snelle opkomst en mondiale verspreiding van digitale technologie en het internet heeft vergaande gevolgen. De bepaling in de Wiv 2002 dat "ongerichte" interceptie van telecommunicatie zich dient te beperken tot "niet-kabelgebonden telecommunicatie" betekent dat het merendeel van alle telecommunicatie zich op dit ogenblik per definitie aan het zicht van de diensten onttrekt. Het wetsvoorstel maakt het mogelijk datastromen ook op de kabel te onderscheppen. Dit is nodig omdat een merendeel van de telecommunicatie zich sinds de invoering van de Wiv 2002 heeft verplaatst van de lucht naar kabelnetwerken, die de ruggengraat zijn gaan vormen van het digitale domein.

De Commissie Dessens heeft daarom aanbevolen de Wiv 2002 techniekonafhankelijk te maken en de beperking in de wet tot "ongericht ontvangen en opnemen van 'niet-kabelgebonden' telecommunicatie" op te heffen. De CTIVD heeft voorts onderstreept dat bij het vaststellen van de Wiv 2002 geen grondrechtelijke reden bestond waarom een bericht dat door de kabel gaat niet mag worden onderschept terwijl datzelfde bericht wel mag worden onderschept als het door de lucht gaat. De CTIVD schrijft in rapport nr. 38:

"De Commissie stelt zich op het standpunt dat het ongericht intercepteren van kabelgebonden telecommunicatie niet op zichzelf reeds een ongeoorloofde inbreuk op de persoonlijke levenssfeer of op een ander grond- of mensenrecht oplevert. Aan de AIVD en de MIVD is immers in de Wiv 2002 een vergelijkbare bevoegdheid toegekend ten aanzien van niet-kabelgebonden telecommunicatie. Bij de totstandkoming van de Wiv 2002 is geen expliciete grondrechtelijke afweging gemaakt over het verschil tussen kabelgebonden en niet-kabelgebonden telecommunicatie. Ook kan niet op voorhand

worden gezegd dat kabelgebonden interceptie, indien voorzien van voldoende waarborgen, op zichzelf in strijd is met het EVRM of andere mensenrechtenverdragen."

Doordat de huidige wet niet techniekonafhankelijk is terwijl de technologie zich onmiskenbaar heeft ontwikkeld, wordt de taakuitvoering van de diensten op dit ogenblik ernstig belemmerd zonder dat dit destijds de bedoeling van de wetgever was. De beperking in de Wiv 2002 betekent dat:

- cyberdreigingen niet tijdig worden onderkend, met potentieel verstrekkende gevolgen voor cybersecurity in Nederland en Europa;
- Nederlandse militairen-op-missie minder goed worden beschermd en ondersteund dan nodig en mogelijk is;
- terroristische activiteiten mogelijk niet tijdig worden onderkend;
- de werkelijke intenties van risicolanden, bijvoorbeeld op het gebied van massavernietigingswapens, verborgen blijven;
- bij snel opkomende crises in het buitenland aanzienlijk minder snel een toereikende informatiepositie kan worden opgebouwd;
- inzet van de krijgsmacht in het digitale domein (zie de Defensie Cyber Strategie) onvoldoende kan worden ondersteund;
- de ontvreemding van hoogwaardige technologische kennis, bedrijfsvertrouwelijke informatie, persoonsgegevens, vitale economische informatie en staatsgeheimen onopgemerkt blijft. De dreigingen in *cyberspace* zijn reëel en raken burgers, bedrijven, overheden en instellingen.

1.3.3. Terroristische dreiging en ondersteuning krijgsmacht

De AIVD verstoort ieder jaar meerdere potentiële terroristische dreigingen, in Nederland en in Europa. Meestal in samenwerking met binnenlandse en buitenlandse partners. Het aantal dreigingen neemt toe en de dodelijke aanslagen binnen Europa zijn schokkend en in potentie maatschappij ontwrichtend. Nationaal en internationaal terrorisme bedreigt de vrije samenleving dan ook op twee manieren. Ten eerste direct door het zaaien van dood en verderf. De tweede bedreiging is indirect, maar soms nog ingrijpender. Terroristische aanvallen veroorzaken angst en kunnen tegenstellingen tussen bevolkingsgroepen verscherpen. Dit kan reacties uitlokken die het democratische, rechtsstatelijke karakter van onze samenleving uithollen.

Ook buiten Europa slaan terroristische organisaties om zich heen. In onder andere Irak en Syrië, maar ook in Noord- en Oost-Afrika worden bijna dagelijks aanslagen gepleegd. In verschillende landen zijn internationale troepenmachten actief om terroristische organisaties te bestrijden en om de internationale rechtsorde te herstellen. Inlichtingen

spelen een cruciale rol bij het succesvol opereren van onze diensten en bij onze militaire en diplomatieke inzet.

Betrouwbare en tijdige inlichtingen zijn daarbij onmisbaar. Dit begint al bij de politieke en internationale besluitvorming over mogelijke missies. Daarbij is een gedegen inzicht in de internationale en lokale veiligheidssituatie, machtsverhoudingen en intenties cruciaal. Ook draagt de MIVD bij aan de effectieve uitvoering van operaties. Denk bijvoorbeeld aan de kleine eenheid van *special forces,* die voor haar veiligheid en het succes van operatie moet kunnen bouwen op betrouwbare en bijna *real-time* aangereikte informatie.

De Nederlandse regering ziet het als prioriteit om het land te beschermen. Tegelijkertijd kiest zij niet voor een samenleving waarin burgers zonder gerechtvaardigde redenen worden gevolgd en in de gaten worden gehouden. Zij wil geen samenleving waarin bepaalde bevolkingsgroepen met achterdocht worden gadegeslagen. Dat past niet bij de democratische rechtsstaat en vrije samenleving die Nederland wil zijn. Deze vrije samenleving én de internationale vrede en veiligheid vergen een actieve rol van de overheid. Vanwege het verwachte langdurige karakter van de huidige terroristische dreiging heeft de regering reeds in februari 2015 onder meer de slagkracht van de AIVD en de MIVD aanzienlijk vergroot door het budget te verhogen oplopend tot € 40 respectievelijk € 17 miljoen per jaar.

1.3.4. Cybersecurity

Nederland wordt vaak geroemd om zijn hoogstaande *high tech* bedrijfsleven. Tegelijkertijd maakt de afhankelijkheid van het internet ons kwetsbaar: vitale sectoren als energie en luchtvaart, telecombedrijven, havens maar ook het regulier bedrijfsleven, het MKB en overheidsorganisaties worden digitaal aangevallen. De huidige cyberdreiging is groot en divers en de verwachting is dat deze nog zal groeien. Dit kan financiële schade veroorzaken, maar door de koppeling met fysieke systemen is daadwerkelijk gevaar voor mensenlevens en grote materiële schade niet louter denkbeeldig. Dit kan schade veroorzaken die ver voorbij louter financieel verlies gaat. De verdediging tegen cyberaanvallen van kwaadwillende mogendheden en buitenlandse organisaties is al een dagelijkse aangelegenheid.

Een substantieel deel van alle systemen in Nederland is geconfronteerd met digitale aanvallen. In het Cybersecuritybeeld Nederland 2015[2] is aangegeven dat de AIVD en de MIVD meerdere digitale spionageaanvallen hebben onderkend, die tal van Nederlandse bedrijven als doelwit hadden. Ook is sprake van de heimelijke verkenningen van

[2] Kamerstukken II 2015/16, 26 643, nr. 369 (bijlage).

systemen binnen de vitale infrastructuur en de overheid. Een deel van deze aanvallen is afkomstig van buitenlandse inlichtingendiensten. De geraakte bedrijven zijn voornamelijk actief binnen de defensie-, *hightech*-, tuinbouw-, chemie-, energie-, en ruimte- en luchtvaartsector. Aangezien bedrijven soms jarenlang niet door hebben dat hun systemen zijn gehackt, is de totale omvang van deze digitale spionageaanvallen op Nederlandse bedrijven en de economische schade als gevolg hiervan niet vast te stellen. Een voorbeeld van de omvang van één enkele recente digitale aanvalscampagne die is onderzocht, laat zien dat er sprake was van meer dan duizend gehackte servers. Nog eens honderd keer zoveel e-mailadressen waren doelwit van de campagne. De aanval was gericht op honderden organisaties wereldwijd, waarvan een deel in Nederland gevestigd.

Bij dit alles is het belangrijk te bedenken dat het vele malen gemakkelijker is om een netwerk aan te vallen dan om het te verdedigen. De overheid is een belangrijke actor die op dit terrein een krachtige vuist kan en moet maken. Zoals in de fysieke wereld de overheid dijken bouwt tegen overstromingen, heeft in de digitale wereld de overheid de capaciteit en de expertise om burgers en bedrijfsleven te beschermen tegen gecompliceerde, grootschalige cyberaanvallen. De overheid kan de tegenactie inzetten door de inzet van legitieme middelen. Juist bij digitale aanvallen geldt, dat nationale zekerheid en nationale veiligheid hand in hand gaan. Zonder economische zekerheid kan nationale veiligheid niet gerealiseerd worden. En zonder nationale veiligheid zal er geen economische zekerheid zijn. Bescherming van het verdienvermogen van Nederland en het ongestoord functioneren van overheid en bedrijfsleven vereist een digitale grensbewaking.

Sommigen bezien de modernisering van de bevoegdheden met argwaan, omdat de overheid hiermee in hun ogen in potentie ongebreidelde toegang zou krijgen tot bedrijfsvertrouwelijke gegevens. De regering ziet dit anders: de modernisering van bevoegdheden is noodzakelijk om ons te beschermen tegen hen die kwaad willen.

1.3.5. Bescherming door inlichtingen- en veiligheidsdiensten: noodzaak van onderzoeksopdrachtgerichte interceptie

Het is de missie van onze inlichtingen- en veiligheidsdiensten om onze samenleving, vitale sectoren, het bedrijfsleven en de overheid te beschermen door dreigingen tegen deze nationale veiligheidsbelangen tijdig te onderkennen. Dat kunnen de diensten alleen als zij bevoegdheden hebben om hun werk te doen in deze digitale wereld. Bevoegdheden die gelijke tred houden met technologische ontwikkelingen. Met dit wetsvoorstel krijgen onze inlichtingen- en veiligheidsdiensten de bevoegdheid om zogenoemde onderzoeksopdrachtgerichte interceptie te verrichten in het kabelgebonden

domein. Dit is essentieel om ook bedreigingen waarover nog geen concrete identificerende gegevens bekend zijn, te onderkennen. *Targets* die er nu in slagen onder de radar te blijven, kunnen toch worden gevolgd. Dat is een belangrijke inhaalslag. Met behulp van onderzoeksopdrachtgerichte interceptie vormen de diensten, in het bijzonder jegens statelijke en *state sponsored* dreigingen, het fundament van de *firewall* rondom Nederland als een veilige plaats om te leven, te werken en zaken te doen.

1.3.6. Internationale verantwoordelijkheid

Nederland is geen eiland. Ook niet op het gebied van *cyber.* Nederland fungeert als internationale *hub* voor datacommunicatie. Dit brengt bijzondere verantwoordelijkheid met zich mee. Interceptie, het vergaren van grote hoeveelheden communicatiegegevens anders dan de bestaande 'tap' die gericht is op een concreet persoon of telefoonnummer, is een praktijk die bij veel buurlanden inmiddels gemeengoed is geworden. Zo beschikken bijvoorbeeld Duitsland, het Verenigd Koninkrijk, Frankrijk en België alle over deze wettelijke bevoegdheid. Buitenlandse partners geven aan dat zij significant meer terroristische aanslagen en cyberaanvallen richting Europa hebben kunnen afwenden door gebruik van onderzoeksopdrachtgerichte interceptie. Ter illustratie: het Verenigd Koninkrijk gaf in 2015 in openbare bronnen aan, dat de analyse van gegevens verkregen door onderzoeksopdrachtgerichte interceptie een significante rol speelde in elk belangrijk onderzoek met betrekking tot contraterrorisme in de voorgaande tien jaar. Daaronder ook de zeven terroristische aanslagen die sinds november 2014 werden voorkomen. 95% van de cyberaanvallen die in een periode van zes maanden waren gedetecteerd door de inlichtingen- en veiligheidsdiensten alleen konden worden ontdekt door inzet van onderzoeksopdrachtgerichte interceptie. Daaronder zaten talloze aanvallen op alle belangrijke bedrijfssectoren en op overheidsnetwerken. In een toenemend aantal gevallen verkrijgen de Nederlandse inlichtingen- en veiligheidsdiensten informatie van hun partnerdiensten over directe dreiging voor Nederland, die zij vanwege de beperkte bevoegdheden zelf niet konden onderkennen. Onze diensten lopen dan soms achter de feiten aan: het kwaad, zoals het stelen van intellectueel eigendom, is geschied. Dit alles maakt duidelijk dat stilstaan geen optie meer is in de digitale wapenwedloop.

Daarnaast is het niet ondenkbaar dat Nederland vanwege de technologisch beperkte interceptiemogelijkheden juist aantrekkelijker wordt voor cyberaanvallers. Misbruik van de Nederlandse infrastructuur berokkent schade aan ons eigen land, maar ook aan andere landen. Het is een evidente plicht dit zoveel mogelijk te voorkomen. Internationale samenwerking is daarom onlosmakelijk verbonden met het inlichtingenwerk. Nederland heeft bovendien concrete internationale verantwoordelijkheden. Het tegengaan van de proliferatie van massavernietigingswapens

is een verdragsrechtelijke verplichting. Nederland zet zich elke dag in voor bevorderen van de internationale rechtsorde. Bij vredesmissies, crisisbeheersings- of andere militaire operaties is bondgenootschappelijke samenwerking fundamenteel. De MIVD draagt op dagelijkse basis bij aan het beschermen van Nederlandse mensenlevens en die van bondgenoten. Ook draagt de MIVD bij aan de effectieve uitvoering van operaties en aan de veiligheid van militaire middelen. Dit laatste verdient meer aandacht dan ooit. Sensor-, wapen- en commandosystemen zijn in toenemende mate complexe digitale systemen. Zonder een goede bescherming tegen manipulatie en verstoring, kan de slagkracht van de krijgsmacht in een ogenblik ernstig verminkt raken. Opgemerkt wordt dat in de kabinetsreactie bij het rapport van de Commissie Dessens is aangegeven dat in het geval van militaire operaties in het buitenland het van toepassing zijnde internationale juridische kader (volkenrechtelijk mandaat) primair de grondslag biedt en kaderstellend is voor het optreden van de MIVD. De Wiv 2002 wordt dan analoog toegepast voor zover de omstandigheden in het operatiegebied dat toelaten. De CTIVD is in het toezichtrapport nr. 44[3] ingegaan op de specifieke militaire omstandigheden in operatiegebied en heeft aangegeven in welke omstandigheden er ruimte moet zijn om van wettelijke procedures af te wijken.

1.4. Nadere achtergronden bij de ontwikkelingen die dit wetsvoorstel noodzakelijk maken

1.4.1. Keuze voor robuuste inlichtingen en veiligheidsdiensten

De regering kiest voor robuuste inlichtingen- en veiligheidsdiensten, die snel, effectief en goed gecontroleerd dreigingen kunnen detecteren en verstoren en andere partijen handelingsperspectief bieden. Terwijl het wezen van onze vrije samenleving onaangetast blijft, moeten onze diensten ook in de toekomst in staat worden gesteld hun noodzakelijke werk uit te voeren. Met het huidige wettelijke kader kan dit niet worden gewaarborgd.

Het niet kunnen onderkennen van de communicatie via nieuwe communicatiemiddelen is naar de mening van de regering dan ook onverantwoord. Het internet is helaas ook het *command and control* systeem van opponenten. Als de omstandigheden hierom vragen, moeten de diensten zich toegang kunnen verschaffen tot relevante communicatie. De snelle ontwikkeling van dreigingen en de evolutie van communicatiemiddelen maakt een snelle inzet van bevoegdheden noodzakelijker dan ooit. Een gerichte, toegesneden inzet is daarbij een uitgangspunt, maar dat is niet altijd mogelijk. Het onderkennen van een nu nog ongekende dreiging vereist dat bevoegdheden in eerste instantie op een ruimere

[3] CTIVD-rapport nr. 44, inzake twee operaties die door de MIVD zijn uitgevoerd ter ondersteuning van de Nederlandse inspanningen op het gebied van piraterijbestrijding in de Hoorn van Afrika.

schaal kunnen worden ingezet dan enkel de personen die al in beeld zijn. De jihadisten of vijandige hackers van vandaag de dag hebben immers geen vast telefoonnummer of clubhuis. Zij bewegen zich vrij door de digitale ruimte.

1.4.2. Chatten is het nieuwe telefoneren

Om de bewegingen van kwaadwillenden te detecteren, zijn nieuwe bevoegdheden nodig. Telefonisch contact is niet langer de norm, maar slechts één van de vele manieren om te communiceren. De opbrengst van de traditionele telefoontap neemt af. Kwaadwillenden wijken steeds meer uit naar open en anonieme toegangspunten van het internet, zoals het wifi-netwerk van een restaurant of een hotel. Zij gebruiken chatfuncties in games en berichten- en videodiensten van sociale media. Dat doen zij doelbewust om onder de radar te kunnen blijven.

1.4.3. De dreiging die we niet kennen

De inlichtingen- en veiligheidsdiensten nemen een unieke positie in. Zij dienen tijdig te onderkennen wat onze nationale veiligheid bedreigt. Deze taak wijkt af van het reguliere opsporingswerk. Ter illustratie: na een aanslag brengen politie en justitie in kaart wat is gebeurd en achterhalen zij de daders. De inlichtingen- en veiligheidsdiensten zullen op grond van wat bekend wordt vlak na de aanslag aanwijzingen verzamelen om een volgende aanslag te kunnen voorkomen. Dit vergt de beschikbaarheid, uit onderzoeksopdrachtgerichte interceptie, van grotere hoeveelheden telecommunicatie. De analyse van historische gegevens, voornamelijk zogenoemde metadata, is hierbij van cruciaal belang. Met wie hebben de aanslagplegers contact gehad? Zijn er meer cellen in Europa en wat zijn hun plannen?

Deze vragen zijn niet te beantwoorden aan de hand van traditionele targetgerichte inlichtingenmiddelen als de telefoontap of microfoon. Juist de dreiging die we niet kennen kunnen we niet onderkennen met traditionele middelen als de telefoontap. Daarvoor is immers een tot de persoon herleidbaar kenmerk nodig. Zo'n kenmerk is niet voorhanden bij ongekende dreiging. En dus moet aanvankelijk op een grotere groep worden ingezet, om uiteindelijk bij de persoon uit te komen die nog niet op de radar verscheen.

Door de kabel vreten digitale virussen en malicieuze software (*malware*) zich in luttele tijd een weg door de Nederlandse ICT-infrastructuur. Nederland leeft van *high tech*; Nederland is een knooppunt van internationale IT. Mede daarom is Nederland een aantrekkelijk doelwit. Met een goed geplaatste hack heb je geen laboratoria of patenten nodig, maar verschaf je jezelf toegang tot *research & development*-opbrengsten die met veel moeite en investeringen zijn opgebouwd.

Van bovenaf gezien lijkt het kabellandschap op onze watervoorziening. Deze vergelijking doortrekkend voor de dreiging die via de kabel tot ons komt, leidt tot de conclusie dat we nu geen waterzuiveringssysteem hebben. We kunnen een filter plaatsen op de wateraansluiting van een enkel huis, namelijk het bedrijf dat meldt dat zijn IT is aangevallen. Maar een systeem waarbij de kwaliteit van het water daar waar nodig kan worden onderzocht bij het binnenkomen van ons land, is er niet. Daarmee rennen we van de ene dreiging naar de andere. Dit is niet meer dan symptoombestrijding en daarmee geen adequate verdediging van het Nederlands belang.

1.4.4. Zekerheid voor de toekomst

De regering wil een goede wettelijke basis voor het noodzakelijke handelen van de inlichtingen- en veiligheidsdiensten. Solide wetgeving die uitgaat van de (juridische) noodzaak om geen onzekerheid te laten bestaan over wat de diensten wel en niet mogen, én die ook bij de snelle technologische ontwikkelingen voldoende basis biedt voor het werk van de diensten. Dat laatste stelt eisen aan de formulering van de bevoegdheden. De regering is daarbij van mening dat nieuwe, ruimere bevoegdheden alleen kunnen worden uitgeoefend als het verder gebruik van de verkregen informatie wordt gereguleerd en er robuuste controle wordt uitgeoefend op inzet van de bevoegdheden en op het verder gebruik van de informatie. Daarom wordt voorzien in goed toegeruste, onafhankelijke controleorganen.

1.5. Hoe heeft de regering het wetsvoorstel voorbereid?

De ontwikkelingen in de digitale wereld gaan ongekend snel en dat vraagt om nieuwe bevoegdheden. De regering is niet de enige die deze conclusie heeft getrokken. In 2011 wees de Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (CTIVD) al op het feit dat de wet interceptie van berichten wel toestaat in de ether, maar niet op de kabel. De CTIVD noemde deze situatie “wat gedateerd”. Datastromen via kabels waren toen al enorm toegenomen vanwege de grote capaciteit van glasvezeltechnologie, en de kabeldichtheid in Nederland was en is groot. De CTIVD kwam met de aanbeveling om onderzoek te doen naar de mogelijkheid en de (juridische) implicaties van een uitbreiding van de interceptiebevoegdheid. De regering was het daar mee eens. De Wiv 2002 was op dat moment al bijna tien jaar oud. De voorbereidingen voor een wetswijziging werden gestart.

Commissie Dessens

Later in 2011 nam de Tweede Kamer de motie Elissen/Çorüz[4] aan, waarin de regering werd gevraagd een evaluatie uit te voeren naar de Wiv 2002. Het kabinet respecteerde deze wens en vroeg een onafhankelijke commissie een onderzoek uit te voeren. Deze Commissie Evaluatie Wiv 2002, ook Commissie Dessens genoemd, ging begin 2013 van start. Op 2 december 2013 verscheen haar rapport. De commissie adviseerde onder meer om interceptie op de kabel mogelijk te maken[5], en om daaraan meer waarborgen te verbinden dan in de Wiv 2002 staan. Het toezicht op de uitvoering van bijzondere bevoegdheden moest steviger, zo bepleitte de commissie.

Internetconsultatie en Privacy Impact Assessment (PIA)

De regering is niet over één nacht ijs gegaan. Tussen het verschijnen van het rapport van de Commissie Dessens en het gereedkomen van deze nieuwe wet ligt tweeënhalf jaar. Het overnemen van het advies van de commissie was op zich niet ingewikkeld. Maar de regering moest handen en voeten geven aan een juiste balans tussen het garanderen van veiligheid en het beschermen van privacy van burgers in een digitale wereld. De regering heeft daarvoor in november 2014 de uitgangspunten op een rij gezet, om de Tweede Kamer de gelegenheid te geven hierop te reageren. In de zomer van 2015 is het concept-wetsvoorstel aangeboden voor een internetconsultatie.

De internetconsultatie heeft zeer veel reacties opgeleverd. Er was instemming met de modernisering van de bevoegdheden. Maar er zijn ook zorgen geuit: zorgen over de inbreuken op de privacy van burgers en zorgen over mogelijk nadeel voor de concurrentiepositie van het Nederlandse bedrijfsleven, met name de telecommunicatiesector. De regering heeft zich vanaf de zomer van 2015 gebogen over deze zorgen. Daarbij is begin 2016 ook een door de Tweede Kamer gevraagde *Privacy Impact Assessment* (PIA) opgeleverd door het onafhankelijke onderzoeksbureau PI.Lab. De resultaten van de consultatie en de PIA zijn verwerkt in het nu voorliggende wetsvoorstel.

In hoofdstuk 12 staat aangegeven welke onderdelen uit deze PIA zijn overgenomen in het voorliggende wetsvoorstel. Ook bevat dit hoofdstuk een overzicht met de belangrijkste onderwerpen die uit de internetconsultatie naar voren zijn gekomen, inclusief de manier waarop die onderwerpen in het voorliggende wetsvoorstel worden geadresseerd.

1.6. Wat verandert er met het nieuwe wetsvoorstel?

[4] Kamerstukken II 2011/12, 29 924, nr. 76.
[5] Ook de Commissie Dessens plaatste deze aanbeveling in de context van de snelle technologische ontwikkelingen van de afgelopen jaren. Zie hiervoor: *Evaluatie Wet op de inlichtingen- en veiligheidsdiensten 2002. Naar een nieuwe balans tussen bevoegdheden en waarborgen*, blz. 70-77 en - waar het cyber betreft - blz. 85-89.

Bijzondere bevoegdheden worden gemoderniseerd door het onderscheid tussen kabelgebonden en niet-kabelgebonden telecommunicatie te vervangen door de zogenoemde onderzoeksopdrachtgerichte interceptie. Dit betekent dat de AIVD en de MIVD telecommunicatie kunnen verwerven, verwerken en analyseren als zij op zoek zijn naar personen, organisaties en dreigingen maar door onvoldoende kennis (nog) niet gericht te werk kunnen gaan. Dat kan alleen met vooraf geaccordeerde onderzoeksopdrachten. Een voorbeeld maakt het inzichtelijk: contacten tussen planners van aanslagen in een land in het Midden-Oosten en Nederlandse sympathisanten worden onderkend door het selecteren van communicatie via de kabel aan de hand van bekende *nicknames* van de planners van aanslagen. De manier waarop onderzoeksopdrachtgerichte interceptie in zijn werk gaat is schematisch weergegeven in bijlage 4. In het schema worden ook de benodigde lastgevingen weergegeven, en de toetsingsmomenten.

De controle op de diensten wordt aanzienlijk versterkt. De modernisering en uitbreiding van de bijzondere bevoegdheden vraagt om een nog sterkere controle. Er komt een Toetsingscommissie Inzet Bevoegdheden (TIB). Dat is een onafhankelijke commissie die bestaat uit drie leden, waarvan ten minste twee leden dienen te beschikken over een ruime rechterlijke ervaring. Het derde lid kan, indien daar behoefte aan is, worden aangezocht vanwege andersoortige expertise, bijvoorbeeld op technisch vlak, die voor een goede taakvervulling van de TIB van belang kan zijn. De TIB zal voortaan de door de minister verleende toestemming voor de uitoefening van bepaalde bijzondere bevoegdheden op rechtmatigheid toetsen *voorafgaand* aan de daadwerkelijke uitoefening van de desbetreffende bevoegdheid; indien de TIB tot het oordeel komt dat de toestemming onrechtmatig is verleend, vervalt de toestemming van rechtswege. Daarnaast hebben burgers de mogelijkheid een klacht in te dienen over het handelen van de AIVD en/of de MIVD. Burgers die dat doen krijgen voortaan een bindende uitspraak van de CTIVD. De minister is dus verplicht het oordeel van de CTIVD op te volgen.

Bestaande, noodzakelijke praktijken van de diensten die nu impliciet onder de wet vallen worden expliciet gemaakt in dit nieuwe wetsvoorstel. Zo wordt duidelijk vastgelegd dat binnentreden in een geautomatiseerd werk (hacken) van een persoon of organisatie die in onderzoek is, ook plaats kan vinden via een geautomatiseerd werk van een derde. Verder gebeurt het opvragen van gegevens tegenwoordig in veel gevallen geautomatiseerd, en de diensten passen data-analyse toe op de datasets die zij op legitieme wijze hebben vergaard. Tevens wordt, naar aanleiding van rapporten van de CTIVD, de praktijk van DNA-onderzoek wettelijk geregeld en wordt voorzien in een grondslag voor het doen van naslag op verzoek van anderen. Tot slot wordt in de wet

vastgelegd dat de verstrekking van ongeëvalueerde gegevens met buitenlandse collegadiensten enkel na toestemming van de betrokken minister kan plaatsvinden. Dit zijn dus nadrukkelijk geen nieuwe bevoegdheden. Het gaat om het vastleggen van bestaande praktijken en de bijbehorende waarborgen.

Naast bovenstaande veranderingen zijn er in dit wetsvoorstel nog enkele wijzigingen aangebracht ten opzichte van de Wiv 2002. De regering wijst op de gewijzigde systematiek voor het aanwijzen van de onderwerpen waarover de regering inlichtingen nodig heeft, en op de samenwerking tussen de beide diensten. De criteria die worden gebruikt voor het aangaan van een samenwerkingsrelatie met een buitenlandse dienst worden geëxpliciteerd. Verder wordt een grondslag gemaakt voor het kunnen vernietigen van gegevens die de identiteit van agenten en informanten zouden kunnen blootgeven. Ook wordt geregeld dat de diensten bijzondere bevoegdheden mogen inzetten om de veiligheid van eigen medewerkers te garanderen of om de betrouwbaarheid van een menselijke bron te kunnen testen. Voor een uitputtende opsomming verwijzen wij naar de navolgende hoofdstukken in deze memorie van toelichting.

1.7. Wat gaan wij nu wel en niet doen in de praktijk?

Ten overvloede merkt de regering op, dat er geen sprake van is dat een fors deel van de telecommunicatie van de Nederlanders zal worden opgeslagen. Wij gaan geen grote klem plaatsen op de GSM-providers in ons land. Wij gaan niet op zoek naar mensen die het woord 'bom' of 'ISIS' gebruiken in hun e-mails. We trekken niet in bulk internetverkeer naar binnen om te kijken welke mensen op zoek zijn naar kunstmest. Wij bekijken niet de Youtube-voorkeuren van Nederlandse burgers.

Wat doen we wel? Onderzoeksopdracht gerichte interceptie zal te allen tijde een zeer klein percentage betreffen van het totaal aan nationaal en internationaal dataverkeer. De regering zal in 2017 één zogenaamde '*access*-locatie' gereedmaken voor onderzoeksopdrachtgerichte interceptie. Het dreigingsbeeld is daarbij bepalend: bezien wordt op welk punt van de Nederlandse infrastructuur zal moeten worden aangehaakt om de noodzakelijke data te kunnen onderscheppen. Daarna zal aan de minister die het betreft en aan de onafhankelijke toetsingscommissie worden verzocht om het middel in te kunnen zetten voor een periode. Dit gebeurt in goed overleg met de telecommunicatiesector. De kosten van het betreffende bedrijf worden vergoed. In de periode daarna wil de regering per jaar, tot 2020, uitbreiden met één 'access locatie'. Zo doen de diensten stapsgewijs ervaring op met inzet en gebruik van dit middel, inclusief het verkrijgen van de benodigde toestemming. De regering verwacht dat hiermee de goede balans is gevonden tussen de noodzakelijke inzet van onderzoeksopdrachtgerichte

interceptie en een verantwoorde schaalgrootte. Evaluatie van het middel is daarbij een - wettelijk verplichte - noodzaak.

1.8. Opbouw van het wetsvoorstel

1.8.1. Thematische opbouw

De huidige wet kent een thematische opbouw. De opbouw van het voorliggende wetsvoorstel sluit daarbij grotendeels aan.

1.8.2. De hoofdstukken kort beschreven

Het wetsvoorstel kent evenals de huidige Wiv 2002 een hoofdstuk 1 met enkele algemene bepalingen (definitiebepalingen en bepaling inzake gebondenheid bij taakuitvoering aan de wet).

Hoofdstuk 2 geeft evenals het huidige hoofdstuk 2 een regeling voor de diensten en de coördinatie (van de taakuitvoering) van de diensten. Een nieuw element daarin vormt de regeling van de zogeheten Geïntegreerde Aanwijzing (GA) (artikelen 5 en 6).

Hoofdstuk 3 vormt het kernstuk van het wetsvoorstel, waarin de kernactiviteit van de diensten wordt geregeld: de verwerking van gegevens. Dit hoofdstuk is qua structuur ietwat aangepast ten opzichte van de structuur in de huidige wet. Dit naar aanleiding van hetgeen in aanbeveling 1 uit de PIA Wiv is aangegeven, waarin is gesteld dat de structuur van de wet helderder en simpeler kan. Zo wordt aldaar voorgesteld om diverse bepalingen die de activiteiten van de diensten in algemene zin normeren bij elkaar te plaatsen in één normeringskader. Daaraan is deels gevolg gegeven. Zo zijn de bepalingen inzake de verwijdering, vernietiging en overbrenging van gegevens (paragraaf 3.4 Wiv 2002) verplaatst naar de paragraaf inzake de algemene bepalingen die aan de *verwerking* van (persoons)gegevens worden gesteld (paragraaf 3.1 van het wetsvoorstel). Waar het gaat om de *verzameling* van gegevens is in de paragraaf 3.2.1 van het wetsvoorstel (algemene bepalingen) een bepaling opgenomen waarin is bepaald uit welke bronnen de diensten bevoegd zijn gegevens te verzamelen (artikel 25). Voorts is de regeling inzake het afwegingskader en de verslaglegging, die in de huidige wet (artikelen 31 tot en met 33) is opgenomen bij de regeling inzake de uitoefening van bijzondere bevoegdheden, naar deze paragraaf verplaatst; het daarin opgenomen afwegingskader is immers in alle gevallen waarin bevoegdheden worden ingezet om gegevens te verzamelen, dus ook waar het niet gaat om bijzondere bevoegdheden, van toepassing.

Het onderscheid tussen algemene en bijzondere bevoegdheden is gehandhaafd met dien verstande dat de aanduiding van de algemene bevoegdheid (huidig artikel 17 Wiv 2002;

artikel 39 wetsvoorstel) in overeenstemming is gebracht met de inhoud daarvan, namelijk de bevoegdheid tot raadpleging van informanten. Daarnaast is ook een expliciete wettelijke grondslag opgenomen voor het stelselmatig verzamelen van gegevens omtrent personen uit open bronnen (artikel 38).

Een geheel nieuwe onderdeel vormt de regeling voor de nieuwe Toetsingscommissie inzet bevoegdheden (TIB); deze onafhankelijke commissie zal voortaan de door de minister verleende toestemming voor de uitoefening van bepaalde bijzondere bevoegdheden op rechtmatigheid toetsen voorafgaand aan de daadwerkelijke uitoefening van de desbetreffende bevoegdheid; indien de TIB tot het oordeel komt dat de toestemming onrechtmatig is verleend, vervalt de toestemming van rechtswege (paragraaf 3.2.2). Met de introductie van de TIB wordt met name tegemoet gekomen aan de kritiek uit de (internet)consultatie dat er niet in een (voorafgaande) onafhankelijke toets zou zijn voorzien en er aldus niet wordt voldaan aan de eisen die uit (de jurisprudentie met betrekking tot) het EVRM zouden voortvloeien.

De regeling van de bijzondere bevoegdheden (paragraaf 3.2.5) bouwt voort op de bestaande regeling inzake bijzondere bevoegdheden en bouwt deze ook in diverse opzichten uit; onder meer door uitbreiding met een aantal bijzondere bevoegdheden (zoals onderzoeksopdrachtgerichte interceptie en DNA-onderzoek) onder gelijktijdige versterking van de waarborgen bij de bestaande bijzondere bevoegdheden.

In het wetsvoorstel is ten opzichte van de huidige wet voorzien in een nieuw hoofdstuk, te weten hoofdstuk 4 (overige bijzondere bevoegdheden van de diensten). De achtergrond daarvoor is dat in het hoofdstuk gegevensverwerking in de huidige wet 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.

Hoofdstuk 5 betreft de kennisneming van door of ten behoeve van de diensten verwerkte gegevens (de inzageregeling); deze is ten opzichte van de huidige regeling vrijwel ongewijzigd gebleven.

In hoofdstuk 6 wordt een regeling gegeven voor de samenwerking tussen inlichtingen- en veiligheidsdiensten (tussen AIVD en MIVD onderling, maar ook met inlichtingen- en veiligheidsdiensten van andere landen) alsmede met andere instanties. Ook dit hoofdstuk bouwt voort op de bestaande regeling, zij het dat deze in substantiële zin – mede als reactie op de aanbevelingen van de Commissie Dessens – is aangevuld. Vergelijk het opnemen van een wegingskader voor het aangaan van relaties met

inlichtingen- en veiligheidsdiensten van andere landen alsmede een meer met waarborgen omgeven regeling inzake het verlenen (en vragen) van ondersteuning en de verstrekking van gegevens in het kader van de samenwerking met buitenlandse collegadiensten.

Hoofdstuk 7 betreft het toezicht, de klachtbehandeling en de behandeling van meldingen inzake vermoedens van misstanden (klokkenluidersregeling). Alle deze drie de taken zijn ondergebracht bij de bestaande Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (CTIVD), zij het daarin wel – met het oog op het borgen van een onbevooroordeelde behandeling – is voorzien in een aparte afdeling toezicht en een afdeling klachtbehandeling. In het kader van de klachtbehandeling zal de afdeling klachtbehandeling van de CTIVD bindende oordelen kunnen gaan geven.

De hoofdstukken 8 (Geheimhouding), 9 (Bonaire, Sint Eustatius en Saba) en 10 (Straf-, overgangs- en slotbepalingen) zijn deels inhoudelijk gewijzigd (zoals codificatie van de jurisprudentie van de Hoge Raad en de Afdeling bestuursrechtspraak van de Raad van State waar het gaat om de omgang met staatsgeheime informatie in rechtsprocedures); deels betreft het (wetstechnische) aanpassingen onder meer in andere wetgeving. Voorts zijn enkele samenloopbepalingen opgenomen.

1.8.3. Bijlagen

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.

In bijlage 2 bij deze memorie van toelichting is de opbouw van het wetsvoorstel weergegeven.

In bijlage 3 wordt een schematisch overzicht gegeven van de bevoegdheden en de waarborgen die ter zake in het wetsvoorstel zijn voorzien.

In bijlage 4 is een schema opgenomen van het werkproces bij onderzoeksopdrachtgerichte interceptie en de bijbehorende waarborgen.

Bijlage 5 geeft ten slotte een schematisch overzicht van de buitenlandse wetgeving met betrekking tot enkele voor dit wetsvoorstel relevante aspecten; in hoofdstuk 10 van de memorie van toelichting is daar in meer beschrijvende zin op ingegaan.

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. 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 opgaat. Op de GA zal in het onderstaande nog afzonderlijk worden ingegaan.

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.[6] 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[7] 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

[6] 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.
[7] CTIVD rapport nr. 36, Vervolgonderzoek naar door de AIVD uitgebrachte ambtsberichten betreffende (kandidaat) politieke ambtsdragers en potentiële leden van de Koninklijke familie.

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.[8] 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.[9] In het verlengde hiervan kan ook de 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.[10] 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 63.

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[11] 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.[12]

[8] 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.
[9] Kamerstukken II 1999/2000, 25 877, nr. 9, p. 14, in combinatie met Kamerstukken II 1999/2000, 25 877, nr. 8, p. 33.
[10] Kamerstukken II 2013/14, 29 924, nr. 104.
[11] De categorie (kandidaat) politieke ambtsdragers betreft kandidaat-ministers en staatssecretarissen en kandidaat-Kamerleden.
[12] Zie in dit verband de CTIVD toezichtsrapporten nr. 29 en 36.

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 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 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.

Met de voorgestelde regeling wordt niet alleen beoogd helderheid te geven over de juridische grondslag voor naslag[13], 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 62, 66 en 67 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

[13] 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).

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 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 veiligheid (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 e 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 92 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. 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 41, derde 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).

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 91, tweede lid, en 92, 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. De verwerking van gegevens, zowel persoonsgegevens als andere gegevens, omvat het hele scala aan handelingen ter zake. In artikel 1, onder f, van het wetsvoorstel is dit als volgt gedefinieerd: elke handeling of elk geheel van handelingen met betrekking tot gegevens, waaronder in ieder geval het

verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens. In hoofdstuk 3 van het wetsvoorstel, evenals in het huidige hoofdstuk 3 van de Wiv 2002, worden met betrekking tot diverse van deze verwerkingsmodaliteiten (in het bijzonder verzamelen, verstrekken, verwijderen en vernietigen) specifieke wettelijke regelingen getroffen, die ertoe strekken om deze activiteiten mede in het licht van de eisen zoals die uit artikel 8 EVRM voortvloeien nader te normeren.

De regeling in hoofdstuk 3 van het wetsvoorstel wijkt in diverse opzichten af van de huidige regeling in de Wiv 2002 alsmede van het concept-wetsvoorstel zoals dat in juli en augustus 2015 in internetconsultatie is gegeven. Naar aanleiding van daartoe strekkende aanbevelingen uit de PIA is de voorgestelde regeling opnieuw tegen het licht gehouden en is geconcludeerd dat deze op onderdelen qua structuur kan worden verbeterd en op andere onderdelen – onder meer in de sfeer van waarborgen bij de te onderscheiden bevoegdheden – kan worden versterkt. Daarmee wordt ook de overzichtelijkheid van de van toepassing zijnde bepalingen op (modaliteiten van) gegevensverwerking verbeterd.

Zo zijn in paragraaf 3.1 de algemene bepalingen geconcentreerd die betrekking hebben op *gegevensverwerking als zodanig*; dat betekent bijvoorbeeld dat de bepalingen inzake de verwijdering, vernietiging en overbrenging van gegevens, die in de huidige wet in een afzonderlijk deel zijn geplaatst, thans zijn opgenomen bij de algemene bepalingen. Ook zijn enkele bepalingen op onderdelen aangevuld (vergelijk de regeling inzake de verwerking van gevoelige gegevens, de opschorting van de vernietiging van gegevens in verband met lopende procedures en de zorgplicht van de hoofden van dienst).

Overzicht van de bepalingen in paragraaf 3.1

Artikel 17	*Algemene bevoegdheid tot verwerking van gegevens*
Artikel 18	*Verwerking voor een bepaald doel, noodzakelijk, in overeenstemming met de wet en op behoorlijke en zorgvuldige wijze*
Artikel 19	*Omschrijving kring van personen waaromtrent gegevens mogen worden verwerkt*
Artikel 20	*Verwijdering en vernietiging van gegevens*

Artikel 21	*Overbrenging van gegevens naar een archiefbewaarplaats*
Artikel 22	*Uitbreiding werking diverse bepalingen naar ambtenaren die op grond van artikel 91 onderscheidenlijk 92 werkzaamheden voor de diensten verrichten*
Artikel 23	*Zorgplicht hoofde van dienst voor geheimhouding van daarvoor in aanmerking komende gegevens en bronnen alsmede de veiligheid van personen waarmee gegevens worden verzameld*
Artikel 24	*Zorgplicht hoofden van dienst voor technische, personele en organisatorische aspecten van gegevensverwerking*

De paragraaf inzake de verzameling van gegevens (paragraaf 3.2), waarbij in de huidige wet nog onderscheid wordt gemaakt tussen "algemeen", lees: de algemene bevoegdheid (artikel 17 Wiv 2002) en de "bijzondere bevoegdheden" (paragraaf 3.2.2 Wiv 2002) is ten opzichte van de huidige wettelijke regeling ingrijpend aangepast. Paragraaf 3.2.1 behelst de diverse *algemene* bepalingen die betrekking hebben op de *verzameling van gegevens als zodanig* (artikelen 25, 26, en 31) alsmede de *algemene* bepalingen die van toepassing zijn op de *uitoefening van bijzondere bevoegdheden* (artikelen 27, 28, 29 en 30). In deze paragraaf zijn – mede naar aanleiding van aanbeveling 1 uit de PIA Wiv – enkele algemene bepalingen, zoals inzake het toe te passen afwegingskader bij de uitoefening van bevoegdheden gericht op verzameling van gegevens alsmede de verslagleggingsplicht, die in de huidige wet bij de regeling inzake de uitoefening van bijzondere bevoegdheden zijn opgenomen (zie de artikelen 32, 33 en 34 Wiv 2002), naar deze nieuwe paragraaf verplaatst. Voorts is voorzien in een regeling van de informatiebronnen waaruit de diensten gegevens mogen verzamelen; op deze wijze worden bronnen die niet als zodanig zijn benoemd alsnog geëxpliciteerd (vgl. PIA Wiv). Nieuw is de opneming van een algemene bepaling ingevolge welke de diensten de verplichting krijgen om met bijzondere bevoegdheden verzamelde gegevens zo spoedig mogelijk op hun relevantie dienen te onderzoeken (artikel 27); deze bepaling strekt ter uitwerking van aanbeveling 12 onder b van de PIA Wiv. Tot slot zijn in de artikelen 28, 29 en 30 de algemene bepalingen die betrekking hebben op de uitoefening van bijzondere bevoegdheden opgenomen; die zien op het toepassingsbereik van de

bijzondere bevoegdheden, de eisen aan een verzoek om toestemming en het toestemmingsregime in enkele bijzondere situaties.

Overzicht van de algemene bepalingen in paragraaf 3.2.1

Artikel 25	*Opsomming informatiebronnen*
Artikel 26	*Afwegingskader (subsidiariteits- en proportionaliteitstoets)*
Artikel 27	*Onderzoek op relevantie*
Artikel 28	*Toepassingsbereik bijzondere bevoegdheden*
Artikel 29	*Toestemmingsduur en inhoud verzoek om toestemming*
Artikel 30	*Toestemmingsregime bijzondere bevoegdheden in bijzondere gevallen*
Artikel 31	*Verslagleggingsplicht*

In paragraaf 3.2.2 van het wetsvoorstel wordt een regeling voorgesteld ten aanzien van een nieuw in te stellen instantie: de Toetsingscommissie inzet bevoegdheden (TIB). Deze onafhankelijke commissie is belast met een rechtmatigheidstoets op de door de minister zelf verleende toestemmingen voor een aantal bijzondere bevoegdheden *voorafgaand* aan de daadwerkelijke uitvoering daarvan. Daarmee wordt voorzien in een nieuwe waarborg bij de uitoefening van de meest ingrijpende bijzondere bevoegdheden.

Paragraaf 3.2.3 geeft een regeling voor het stelselmatig verzamelen van gegevens uit open bronnen; paragraaf 3.2.4 voor de raadpleging van informanten (het huidige artikel 17 Wiv 2002). Deze bevoegdheden mogen in het kader van alle taken van de diensten worden ingezet. Aansluitend wordt in paragraaf 3.2.5 de bijzondere bevoegdheden van de diensten geregeld. In bijlage 3 van deze memorie van toelichting worden de diverse bevoegdheden van de diensten schematisch gepresenteerd; daarbij is ook aangegeven met welke waarborgen de uitoefening daarvan is omgeven.

Paragraaf 3.2.6 (artikel 59) regelt de notificatieplicht. Deze regeling is ten opzichte van de huidige regeling in paragraaf 3.2.3 (artikel 34) van de Wiv 2002 slechts in beperkte mate gewijzigd.

Paragraaf 3.3 (artikel 60) is ten opzichte van de huidige wet nieuw en geeft een regeling voor diverse vormen van gegevensverwerking die zijn samen te brengen onder de noemer “geautomatiseerde data-analyse”.

Tot slot wordt in paragraaf 3.4 de verstrekking van gegevens – zowel intern als extern – geregeld. Deze regeling is ten opzichte van de bestaande regeling in paragraaf 3.3. van de Wiv 2002 voor een groot deel ongewijzigd gebleven. De belangrijkste aanvullingen ten opzichte van de huidige regeling betreffen: (1) de (procedure rond de) verstrekking van gegevens in het kader van de naslagprocedure (de naslag is in de artikelen 8 en 10 van het wetsvoorstel als een afzonderlijk taakelement voor beide diensten opgenomen) en (2) de verstrekking van ongeëvalueerde gegevens in het kader van een goede taakuitvoering ingeval daartoe een dringende en gewichtige reden bestaat.

In het onderstaande zal thans nader worden ingegaan op de hiervoor geschetste onderdelen.

3.2 De algemene bepalingen inzake de verwerking van gegevens

3.2.1 Algemeen

In paragraaf 3.1 (de artikelen 17 tot en met 24) van het wetsvoorstel zijn de bepalingen geconcentreerd die in algemene zin van toepassing zijn op de verwerking van gegevens[14] door de diensten; deze bepalingen corresponderen (grotendeels) met de huidige artikelen 12 tot en met 16, aangevuld met de bepalingen inzake de verwijdering, vernietiging en overbrenging van gegevens, die thans in paragraaf 3.4 van de huidige wet zijn ondergebracht. Daarmee is deels uitvoering gegeven aan aanbeveling 1 uit de PIA Wiv; de bepalingen die de uitoefening van bijzondere bevoegdheden in algemene zin normeren zijn niet – zoals in de PIA voorgesteld - in dit algemeen normeringskader opgenomen, maar in de paragraaf met algemene bepalingen voor de verzameling van gegevens.

3.2.2 De bevoegdheid tot gegevensverwerking

In artikel 17 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.

3.2.3 Algemene eisen aan gegevensverwerking

[14] Onder gegevens worden hier zowel persoonsgegevens als andere gegevens verstaan (artikel 1, aanhef en onder d).

Aan de gegevensverwerking worden in artikel 18, eerste tot en met derde lid, een aantal eisen gesteld.

Artikel 18, eerste lid, van het wetsvoorstel bevat een algemene normering ten aanzien van de verwerking van gegevens door de diensten. Artikel 18, eerste lid, bepaalt dat de verwerking van gegevens slechts plaats vindt voor een bepaald doel en slechts voor zover dat noodzakelijk is voor een goede uitvoering van de Wet op de inlichtingen- en veiligheidsdiensten of de Wet veiligheidsonderzoeken. Het betreft een bestaande norm welke in huidige Wet op de inlichtingen- en veiligheidsdiensten 2002 in artikel 12, tweede lid, is geregeld en ook daarvoor was opgenomen in de Privacyregelingen van de diensten.

Bij de onderzoeken uitgevoerd door de diensten speelt deze norm een belangrijke rol. Het uitgangspunt is dat de diensten gegevens steeds doelgericht vergaren en verwerken. Ten aanzien van het afwegingskader dat de diensten in het kader van deze norm dienen te hanteren kan het volgende worden opgemerkt. Verwerking van gegevens door de diensten zal uiteraard op de eerste plaats dienen te passen binnen de wettelijke taakomschrijving van de diensten. Daarnaast dient de verwerking van de gegevens door de diensten nodig te zijn voor een goede taakuitvoering. In geval van inzet van bijzondere bevoegdheden zullen de diensten ingevolge artikel 29, tweede lid, van het wetsvoorstel in een verzoek om toestemming niet alleen het onderzoek dienen te verantwoorden waarvoor de betreffende bevoegdheid moet worden uitgeoefend, maar voorts ook het met de uitoefening van de bijzondere bevoegdheid beoogde doel. Bij de keuze van bevoegdheden moet voorts rekening worden gehouden met de vereisten van subsidiariteit en proportionaliteit. Dit betekent dat slechts die bevoegdheden mogen worden ingezet die het minste nadeel opleveren en voorts dat een bevoegdheid niet wordt toegepast indien de uitoefening in vergelijking met het na te streven doel onevenredig nadeel oplevert.

Met betrekking tot de (verdere) verwerking van gegevens door de diensten is het van belang op te merken dat de eis dat informatie voor een bepaald doel wordt vergaard, niet wil zeggen dat deze informatie louter en alleen voor dat doel (verder) mag worden gebruikt. Het verdere gebruik is ook van essentieel belang voor de diensten. Bepalend is dat verdere verwerking noodzakelijk is voor een goede taakuitvoering van de diensten. Zo is deze norm te vinden in de artikelen welke zien op een bijzondere vorm van verdere verwerking, nl. de (interne en externe) verstrekking van gegevens. Aan de hand van een aantal voorbeelden kan worden geconcretiseerd waaraan moet worden gedacht bij (verdere) verwerking welke noodzakelijk is in het kader van een goede taakuitvoering.

Uit een onderzoek naar een geradicaliseerde groep jongeren blijkt één van hen een vertrouwensfunctie te bekleden. In zo'n geval worden die inlichtingen verkregen uit een onderzoek op basis van de a-taak uiteraard verder gebruikt in het kader van het verrichten van een veiligheidsonderzoek op basis van de b-taak.

Uit een onderzoek naar massavernietigingswapens blijkt dat een agent van een buitenlandse dienst een actieve rol speelt in Nederland. Deze agent regelt contacten tussen een Nederlands bedrijf dat dual-use goederen levert aan een land dat zich bezig houdt met het vervaardigen van massavernietigingswapens. Aldus levert het in eerste instantie op het buitenland gerichte onderzoek naar de verspreiding van massavernietigingswapens en het potentieel van een vreemde mogendheid waardevolle startinformatie op voor een onderzoek in het kader van contraspionage in Nederland.

Een ander voorbeeld betreft informatie welke uit een inlichtingenonderzoek voortvloeit en welke relevant is voor cybersecurity. Dit kan informatie zijn waarvan een goede taakuitvoering van de diensten met zich brengt dat deze gedeeld wordt met het NCSC of bedrijven.

Uit deze voorbeelden blijkt dat gegevens die voor een onderzoek in de ene taak zijn vergaard tevens van belang kunnen zijn voor andere onderzoeken binnen dezelfde taak of ook voor een onderzoek binnen een andere taak. Dit geldt binnen de AIVD respectievelijk MIVD en tussen de diensten onderling. De (inter)nationale veiligheidssituatie vraagt immers om een zeer nauwe samenwerking tussen de Nederlandse diensten.

In relatie tot verkregen gegevens door middel van inzet van bijzondere bevoegdheden is voorts nog van belang hetgeen de CTIVD heeft opgemerkt op blz. 29 van het toezichtsrapport nr. 38 inzake gegevensverwerking op het gebied van telecommunicatie door de AIVD en de MIVD. Gegevens die door middel van een bijzondere bevoegdheid worden verkregen, worden met een specifiek doel verworven. Dat doel dient gelegen te zijn binnen de inlichtingen- of veiligheidstaken van de diensten en te worden vastgelegd in de motivering van het verzoek om toestemming. De ruwe opbrengst van de inzet van een bijzondere bevoegdheid mag alleen worden aangewend in het kader van het onderzoek waarbinnen de gegevens zijn verworven of ten behoeve van een ander lopend onderzoek dat onder de inlichtingen- of veiligheidstaken van de diensten valt. Wanneer de gegevens eenmaal geëvalueerd zijn, mogen zij vervolgens in het kader van alle taken van de diensten (dus ook andere dan de inlichtingen- en veiligheidstaken) worden aangewend. Deze lijn stelt enerzijds grenzen aan het gebruik van uit de inzet van bijzondere bevoegdheden verkregen gegevens, maar laat anderzijds ook de ruimte voor

verder gegevensgebruik welke essentieel is voor de goede taakuitvoering van 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 en gelden ook waar het gaat om gegevensverwerking door de diensten. Het criterium behoorlijk biedt, zoals uiteengezet in rapport 38 van de CTIVD (pag. 58), een aanknopingspunt voor een proportionaliteitsvereiste, zoals artikel 8 EVRM vereist, bij alle vormen van gegevensverwerking. Evenredigheid van het middel ten opzichte van het doel is één van de normen van behoorlijk overheidsoptreden.

Waar het gaat om gegevensverwerking door de inlichtingen- en veiligheidsdiensten is in het derde 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.). Niet elke bron en daarmee het aldus verkregen gegeven is echter zonder meer betrouwbaar. Gegevens verkregen door toepassing van technische bronnen, zoals een gerichte tap op een target, zijn over het algemeen als erg betrouwbaar te kwalificeren. De kwalificatie van de betrouwbaarheid van gegevens verkregen van agenten of informanten wordt echter in belangrijke mate mede bepaald door de mate waarin de agent of informant als zodanig als betrouwbaar wordt beoordeeld; dat is afhankelijk van diverse factoren, zoals bijvoorbeeld dat verstrekte gegevens door gegevens uit andere bronnen worden bevestigd. Gelet op het gebruik dat van deze gegevens kan worden gemaakt – bijvoorbeeld als basis voor een mededeling als bedoeld in artikel 62 jo. 68 van het wetsvoorstel) – en de gevolgen die dat kan hebben voor personen of organisaties waarop die gegevens betrekking hebben, is het dan ook van groot belang dat expliciet wordt vastgesteld wat de kwaliteit van die gegevens is.

In het kader van de PIA Wiv[15] is erop gewezen dat het toevoegen van een betrouwbaarheidsaanduiding of bronverwijzing als hier bedoeld, ook houvast zou moeten geven voor de beoordeling van afgeleide gegevens die bijvoorbeeld volgen uit nadere analyse of samenvoeging van de oorspronkelijke gegevens. Men wijst er daarbij tegelijkertijd op dat het nog maar de vraag is of bij de toepassing van bepaalde technologieën, zoals *data mining*, of een aanduiding van de oorspronkelijke

[15] Zie paragraaf 4.2.4 en aanbeveling 26.

betrouwbaarheid (van de verwerkte gegevens) een voldoende waarborg biedt tegen foute interpretaties. Bij het samenvoegen van verschillende gegevensbestanden ontstaat immers een vermenging van bronnen waarbij gegevens in een ander licht komen te staan en uit hun context kunnen worden getrokken, terwijl ook de verschillen tussen de oorspronkelijke bestanden qua betrouwbaarheid van invloed kunnen zijn op de inschatting van de betrouwbaarheid van het resultaat. De PIA beveelt daarom ook aan om naast de bronaanduiding verplicht te documenteren welke analysemethoden zijn gebruikt, alsmede de betrouwbaarheid van deze methode. De in de PIA Wiv geschetste problematiek en de daaraan verbonden risico's worden onderschreven. Het gaat naar ons oordeel echter te ver om zoals in aanbeveling 26 van de PIA Wiv is opgenomen, over te gaan tot het opnemen van een bepaling omtrent betrouwbaarheids- of bronaanduiding van de programmatuur waarmee gegevensverzamelingen worden geanalyseerd. Deze duiding behoort tot de kwaliteit van de bedrijfsvoering van de diensten. De diensten geven bij de programmatuur voor analyses de betrouwbaarheid en de bronaanduiding van de gegevensverzamelingen aan. Tevens is als extra waarborg opgenomen dat het bevorderen of treffen van maatregelen jegens een persoon uitsluitend naar aanleiding van geautomatiseerde data-analyse niet is toegestaan (artikel 60, derde lid).

In artikel 22, 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 91 onderscheidenlijk 92 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 22, 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 22, derde lid, wordt de Minister van BZK onderscheidenlijk de Minister van Defensie aangewezen als zorgdrager voor de bij de artikel 91 onderscheidenlijk 92 berustende archiefbescheiden, voor zover die nog niet naar een rijksarchiefbewaarplaats zijn overgedragen.

3.2.4 De kring van personen

Artikel 19 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 19, derde en vierde lid, is een regeling opgenomen voor de verwerking van gevoelige persoonsgegevens. In de huidige wet worden daartoe gerekend: gegevens betreffende iemands godsdienst of levensovertuiging, ras, gezondheid en seksuele leven. Overeenkomstig aanbeveling 26 van de PIA Wiv is in het wetsvoorstel thans ook het lidmaatschap van een vakvereniging als gevoelig gegeven toegevoegd. Onder een vakvereniging wordt in dit verband, overeenkomstig de door het CBS gehanteerde definitie, verstaan: een vereniging van werknemers die zich ten doel stelt de collectieve en/of individuele belangen van de leden te behartigen bij hun werkgever of bij instanties die invloed op de arbeidsvoorwaarden uitoefenen. 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 18, eerste lid, neergelegde noodzakelijkheidscriterium.[16] 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 18, eerste lid, dat het noodzakelijk is voor een goede uitvoering van de Wiv of de Wvo. Ten

[16] 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.

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 13, eerste lid, onder e, en tweede lid, onder e, van de huidige wet (overgenomen in het wetsvoorstel): 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 de PIA Wiv (blz. 39 en 40) is ook bij deze aanvulling stilgestaan, met name in relatie tot de bevoegdheden waarbij grote hoeveelheden gegevens (bulk) worden verzameld. Geconcludeerd wordt dat het weliswaar problematisch is in het licht van de privacyrisico's voor de personen over wie (onvermijdelijk onterecht) gegevens worden verzameld alsmede in het licht van Weber en Saravia[17], dat vereist dat de categorie van personen die onderworpen kunnen worden aan heimelijke gegevensverzameling moeten worden gedefinieerd; het gaat immers hier feitelijk om iedereen. Tegelijk, aldus de onderzoekers, kan niet worden ontkend dat het moeilijk is de categorie personen nauwkeuriger te omschrijven dan in het vijfde lid gebeurd. Wel achten zij het noodzakelijk dat er compenserende maatregelen worden genomen, bijvoorbeeld door een verplichting niet relevante gegevens zo snel mogelijk te verwijderen; de gehanteerde bewaartermijnen achten zij in dit licht dan ook problematisch. Voor wat betreft de bewaartermijnen, wordt verwezen naar hetgeen ter toelichting op artikel 27 van het wetsvoorstel is gesteld.

3.2.5 De verwijdering, vernietiging en overbrenging van gegevens

In de artikelen 20 en 21 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 vrijwel ongewijzigd is overgenomen; artikel 20 is – ten opzichte van de bestaande regeling – aangevuld met een voorziening die er toe strekt om hangende een klacht- of bezwaarprocedure of een procedure bij een rechter de vernietiging van daarvoor in aanmerking komen gegevens op te schorten.

[17] EHRM 29 juni 2006, *Weber en Saravia t. Duitsland*.

In algemene zin geldt dat gegevens, die gelet op het doel waarvoor zij worden verwerkt, hun betekenis hebben verloren, dienen te worden verwijderd (artikel 20, 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.[18] 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 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 69 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 moet daarvan zo spoedig mededeling worden gedaan (artikel 20, 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 20, vierde lid, is – evenals in de huidige wet - 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 76 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 76, 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. In de PIA Wiv (blz. 50, voetnoot 33) is er op gewezen dat het onwenselijk zou kunnen zijn dat

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

gegevens tussentijds door de diensten worden vernietigd ingeval er een klachtprocedure zou lopen. Dat geldt echter evenzeer waar het gaat om aanhangige bezwaarprocedures of bij aanhangige procedures bij een rechter, dan wel indien er beroep openstaat tegen een uitspraak die in zodanige procedure is gedaan. In artikel 20, vijfde lid, wordt ter zake voorgesteld de vernietiging van voor deze procedures van belang zijnde gegevens op te schorten tot ten minste het moment waarop de klacht of het bezwaar dan wel de rechterlijke uitspraak onherroepelijk is geworden.

Artikel 21 van het wetsvoorstel geeft een bijzondere regeling voor de overbrenging van archiefbescheiden naar een archiefbewaarplaats. Deze regeling is ten opzichte van de bestaande regeling ongewijzigd gebleven.

Met betrekking tot de actuele stand van zaken met betrekking tot de selectielijsten van de AIVD en de MIVD kan overigens nog het volgende worden opgemerkt. De ontwerp-selectielijst voor de AIVD en MIVD zijn, gelet op eerdere toezeggingen, bij brief van 15 december 2015 door de Minister van OC&W, mede namens de Ministers van BZK en Defensie aangeboden aan de Voorzitter van de Tweede Kamer (Kamerstukken II 2015/16, 33 820, nr. 6). Op verzoek van de vaste Kamercommissie van OC&W heeft op 28 januari 2016 een technische briefing plaatsgevonden. De selectielijsten zijn bij besluit van 25 maart 2016 van de ministers van OC&W, BZK en Defensie vastgesteld.[19]

3.2.6 Zorgplichten voor de diensthoofden

In de artikelen 23 en 24 wordt aan de hoofden van de diensten enkele zorgplichten opgelegd; deze verplichtingen komen vrijwel 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 23 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

[19] Stcrt. 2016, nr. 20699 (25 april 2016).

daaraan ontleende gegevens worden (verder) verstrekt, dan stuit vermelding van die bron niet op bezwaren.

Artikel 24 is ten opzichte van de huidige regeling aangevuld met een nieuw eerste lid. Daarin wordt bepaald dat de hoofden van dienst er (voorts) voor zorg dragen dat de technische, personele en organisatorische maatregelen in verband met de verwerking van gegevens in overeenstemming zijn met hetgeen bij of krachtens deze wet is bepaald. Deze bepaling is opgenomen naar aanleiding van aanbeveling 3 in de PIA Wiv om een bepaling op te nemen over gegevensbescherming *by design* en *by default*. Naar ons oordeel kan een dergelijke bepaling aangewezen zijn, indien de verantwoordelijke voor de gegevensverwerking zelf veel ruimte is gelaten om met het oog op dienst taak- of doelstelling de wijze waarop hij gegevens verwerkt (in zijn diverse aspecten) invulling te geven en daarbij de in geding zijnde privacyrisico's te minimaliseren. In het wetsvoorstel is echter een vrij specifiek kader voor diverse aspecten van gegevensverwerking opgenomen, waarbij in de afweging de privacyrisico's – uitgewerkt in diverse waarborgen - reeds zijn meegewogen.

Het verwerken van (persoons)gegevens is, zoals eerder aangegeven, de *core business* van de diensten. Het is daarbij onvermijdelijk dat er grote hoeveelheden gegevens worden verwerkt (big data), waarvan – conform de eisen die daaraan worden gesteld – zo snel mogelijk de relevantie moet worden vastgesteld (datareductie). Dat is niet alleen noodzakelijk om de inbreuk op de privacy tot het noodzakelijke te beperken, maar ook omdat de diensten de focus zo snel mogelijk willen richten op die gegevens die voor het onderzoek daadwerkelijk nodig zijn. Het proces van het vaststellen van de relevantie van gegevens is echter een gecompliceerd proces, dat zich naar ons oordeel niet louter – althans niet nauwkeuriger dan wat het wetsvoorstel ter zake bepaalt – laat vertalen in in technische systemen in te bouwen waarborgen, waarmee wordt bewerkstelligd dat zo min mogelijk persoonsgegevens worden verwerkt. Dat veronachtzaamt de menselijke component; zie ook hetgeen ter zake is opgemerkt bij de bevoegdheid tot geautomatiseerde data-analyse. Waar het gaat om het op een privacy-vriendelijke manier inrichten van de systemen, wordt voorts opgemerkt dat binnen inlichtingen- en veiligheidsdiensten, juist vanwege de aard van de daar verwerkte gegevens en de onderkende privacygevoeligheid ervan, de gehanteerde informatiesystemen standaard zijn voorzien van daarin ingebouwde autorisatieprocedures; daarnaast worden diverse andere, zowel fysieke (vgl. compartimentering binnen het gebouw), organisatorische en personele beschermingsmaatregelen (vgl. functiescheiding), getroffen. Daardoor wordt bewerkstelligd dat de gebruikers van de systemen alleen toegang hebben tot bij die informatie die voor hun taakuitvoering noodzakelijk is. Gelet op het voorgaande achten wij het opnemen van een specifieke bepaling die waarborgt dat gegevensbescherming in

het technische ontwerp van systemen wordt ingebouwd, niet aangewezen. Naar ons oordeel kan volstaan worden met een bepaling, waarbij het hoofd van de dienst de plicht opgelegd krijgt om te zorgen dat de technische, personele en organisatorische maatregelen in verband met de verwerking van gegevens in overeenstemming zijn met hetgeen bij of krachtens de wet is bepaald.

Waar het gaat om de in artikel 24, tweede lid, neergelegde zorgverplichtingen, 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"[20] – in de regeling van een aantal bijzondere bevoegdheden op het vlak van interceptie een vergelijkbare bepaling is opgenomen (zie de artikelen 47, vijfde lid, 48, vierde lid, 49, 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

In paragraaf 3.2 van het wetsvoorstel wordt een regeling gegeven voor de verzameling van gegevens. In paragraaf 3.2.1 zijn een aantal algemene bepalingen geformuleerd; deze zijn deels nieuw (artikelen 25, 27 en 30) en deels bestaand maar aangepast (artikelen 26, 28, 29 en 31[21]). Geheel nieuw – ook ten opzichte van in consultatie gegeven concept-wetsvoorstel – is de regeling voor de Toetsingscommissie inzet bevoegdheden (paragraaf 3.2.2). Mede in reactie op hetgeen in de PIA Wiv is gesteld omtrent het verzamelen van gegevens uit open bronnen is in paragraaf 3.2.3 (artikel 38) de (bestaande) bevoegdheid van de dienst tot het stelselmatig verzamelen van gegevens uit open bronnen geëxpliciteerd. De bestaande bevoegdheid ex artikel 17 Wiv 2002 tot het mogen raadplegen van informanten (thans ook vaak aangeduid als de algemene bevoegdheid) komt terug in paragraaf 3.2.4 (artikel 39) van het wetsvoorstel; ten opzichte van de bestaande regeling is deze op diverse onderdelen aangepast. Paragraaf 3.2.5 (artikelen 40 tot en met 58) bevat ten slotte een regeling van de zogeheten bijzondere bevoegdheden van de diensten; deze regeling is limitatief van karakter.

3.3.2 Algemene bepalingen inzake de verzameling van gegevens

[20] 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.
[21] Zie de artikelen 18, 19, 31, 32 en 33 Wiv 2002.

3.3.2.1 De informatiebronnen van de diensten

In de huidige wet is geen opsomming opgenomen van de informatiebronnen waaruit de diensten gegevens kunnen verzamelen. Slechts impliciet, zie het huidige artikel 31, eerste lid, Wiv 2002 wordt daar (deels) aan gerefereerd: de uitoefening van een bijzondere bevoegdheid is slechts 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*. Ook in de PIA Wiv wordt daarop gewezen.[22] In het wetsvoorstel is ervoor gekozen om de informatiebronnen, waaruit dan wel met behulp waarvan de diensten in ieder geval gegevens kunnen verzamelen, te benoemen (artikel 25, eerste lid). Wel is daarbij voorzien in de mogelijkheid dat de voor de dienst verantwoordelijke minister, indien de onder hem ressorterende dienst het noodzakelijk acht gegevens te verzamelen uit een andere informatiebron als bedoeld in het eerste lid, hij op een daartoe strekkend verzoek van het hoofd daarvoor toestemming kan verlenen (artikel 25, tweede lid). Aldus wordt voor het geval dat zich in de toekomst ook andere voor de dienst relevante informatiebronnen aandienen, die thans (nog) niet zijn (te) voorzien, de mogelijkheid gecreëerd deze te gebruiken. Het ligt voor de hand vanuit de actieve inlichtingenplicht jegens het parlement dat deze omtrent een dergelijke beslissing van de minister wordt geïnformeerd.

De informatiebronnen waaruit dan wel met behulp waarvan de diensten – met inachtneming van het bepaalde bij of krachtens de wet – in ieder geval gegevens mogen verzamelen zijn:

a. *voor een ieder toegankelijke informatiebronnen.* Het gaat hier om alle bronnen (traditionele media, internet e.d.) die zonder meer kunnen worden geraadpleegd en waarvoor geen drempels bestaan.

b. *informatiebronnen waarvoor aan de dienst een recht op kennisneming van de aldaar berustende gegevens is verleend.* Daarbij moet worden gedacht aan bijvoorbeeld commercieel beschikbaar gestelde gegevens, waarbij men slechts tegen betaling toegang toe krijgt (vgl. onder meer de gegevens van de Kamer van Koophandel); maar ook aan gegevens, waarbij de diensten een wettelijk recht op toegang is verleend (vgl. onder meer artikel 17 en 24 Wet politiegegevens).

c. *de raadpleging van informanten als bedoeld in artikel 39.*

[22] Zie paragraaf 5.2.2. PIA Wiv.

d. *de uitoefening van bijzondere bevoegdheden als bedoeld in paragraaf 3.2.5 van het wetsvoorstel.* Bijzondere bevoegdheden zijn alleen toepasbaar bij de uitvoering van de in artikel 8, tweede lid, onder a en d, en 10, tweede lid, onder a, c en e, van het wetsvoorstel aan de AIVD onderscheidenlijk MIVD opgedragen taak. Bevoegdheden die uitgeoefend kunnen worden bij alle taakonderdelen, kunnen aangemerkt worden als algemene bevoegdheden tot gegevensverzameling.

e. *in het kader van de samenwerking tussen inlichtingen- en veiligheidsdiensten en met andere instanties.* In het kader van de samenwerking tussen inlichtingen- en veiligheidsdiensten, zowel tussen AIVD en MIVD als met buitenlandse collegadiensten, worden vele gegevens over en weer verstrekt; het wetsvoorstel biedt daar een afzonderlijke wettelijke grondslag voor. Voorts wordt door de diensten met diverse instanties samengewerkt; deels hebben die een structureel karakter en is deze wettelijk verankerd, waarvan ook de verstrekking van gegevens deel uitmaakt.

De verzameling van gegevens door de diensten vindt plaats *met inachtneming van het bepaalde bij of krachtens de wet.* Deze clausulering hangt samen met het feit dat het gebruik van bepaalde informatiebronnen, met name die waarbij sprake is van het gebruik van bijzondere bevoegdheden, is beperkt tot bepaalde taakonderdelen van de diensten. Ook zijn aan het gebruik van die bevoegdheden veelal nadere, daarop toegesneden eisen gesteld. Waar niet van een dergelijke clausulering sprake is, kunnen de genoemde bronnen voor alle taakonderdelen van de diensten worden ingezet. Zo kunnen bijvoorbeeld ten behoeve van een veiligheidsonderzoek door een dienst ter uitvoering van de Wet veiligheidsonderzoeken (Wvo) openbare bronnen worden geraadpleegd (waaronder informatie op de openbaar toegankelijke delen van het internet, van Facebook, Twitter, LinkedIn e.d.), maar ook informanten worden geraadpleegd.

Het is voorts goed om erop te wijzen dat naast het verrichten van specifieke onderzoeken op grond van de aan de diensten in artikel 8 (AIVD) en 10 (MIVD) opgedragen taken, de diensten met het oog op en ter ondersteuning van een goede taakuitvoering in zijn algemeenheid ook allerlei relevante ontwikkelingen waar ook ter wereld volgen via diverse media (kranten, tijdschriften, internet e.d.) en daarover gegevens vastleggen; bijvoorbeeld voor het opstellen van landenoverzichten, het volgen van politieke ontwikkelingen e.d. Het kennisnemen van vrijelijk verkrijgbare informatie ten behoeve van dit soort - veelal - ondersteunende activiteiten is niet aan een specifieke normering verbonden, zoals bij het verrichten van specifieke onderzoeken op grond van de aan de diensten opgedragen taken.

3.3.2.2 Het afwegingskader bij de uitoefening van de bevoegdheden tot verzameling van gegevens

In artikel 26 van het wetsvoorstel wordt een regeling gegeven voor het bij de uitoefening van bevoegdheden toe te passen afwegingskader. Het gaat dan met name om de zogeheten subsidiariteits- en proportionaliteitstoets. Deze criteria zijn in de jurisprudentie van het EHRM ontwikkeld en indertijd in de Wiv 2002 toegespitst op de bijzondere bevoegdheden gecodificeerd (artikel 31 en 32 Wiv 2002); in de toezichtspraktijk van de CTIVD vormen deze criteria, naast andere, een belangrijk toetssteen. Overigens zou ook zonder een dergelijke codificatie deze toets bij de toepassing van bevoegdheden die een beperking opleveren van bijvoorbeeld het in artikel 8 EVRM neergelegde recht op eerbiediging van privé-, familie- en gezinsleven dienen plaats te vinden. Dat geldt niet alleen voor de bevoegdheid tot gegevensverzameling, maar evenzeer bij andere vormen van gegevensverwerking zoals bijvoorbeeld de uitoefening van de bevoegdheid tot verstrekking van gegevens.

In het concept-wetsvoorstel zoals dat in consultatie is gegeven waren de desbetreffende bepalingen (eveneens) uitsluitend van toepassing verklaard op bijzondere bevoegdheden. In het voorliggende wetsvoorstel wordt de koppeling met bijzondere bevoegdheden losgelaten en wordt het (geëxpliciteerde) afwegingskader nadrukkelijk ook van toepassing verklaard op andere dan bijzondere bevoegdheden, welke beschikbaar zijn in het kader van de verzameling van gegevens. Immers, met de uitoefening van de bevoegdheid tot verzameling van gegevens uit openbare informatiebronnen kan sprake zijn van een beperking van het in artikel 8 EVRM neergelegde recht en in concrete gevallen ten opzichte van andere ter beschikking staande bevoegdheden als niet subsidiair of disproportioneel worden aangemerkt, zeker indien die bevoegdheidsuitoefening een stelselmatig karakter draagt. In de praktijk zal echter het afwegingskader vooral van belang zijn wanneer voor het verkrijgen van bepaalde gegevens de uitoefening van bijzondere bevoegdheden in beeld komt.

In artikel 26, eerste lid, van het wetsvoorstel is de subsidiariteitstoets uitgewerkt. Zoals uit de opsomming van de bevoegdheden in artikel 25 blijkt komen de diensten – mede afhankelijk van de aan de orde zijnde taak[23] - diverse mogelijkheden toe tot het verzamelen van gegevens. Welke gegevens de diensten noodzakelijk achten te verzamelen zal in de praktijk primair worden bepaald door het onderzoeksonderwerp, het doel van het onderzoek, de reeds beschikbare informatie en dergelijke. Afhankelijk van het verloop van het onderzoek en de gegevens die daarin beschikbaar komen, zal telkens dienen te worden bezien welke informatie nog ontbreekt en op welke wijze de

[23] In verband hiermee is de clausule "met inachtneming van het bepaalde bij of krachtens deze wet" relevant.

ontbrekende informatie zou kunnen worden verzameld. Het is met andere woorden een dynamisch proces. Voorts zijn ook aspecten als urgentie mede bepalend bij de te maken keuze. Bij de te maken toets op grond van artikel 26, eerste lid, spelen deze factoren allemaal een rol. Echter uiteindelijk zal die bevoegdheid (of combinatie van bevoegdheden) dienen te worden gekozen die voor de betrokkene – dat wil zeggen degene jegens wie de bevoegdheid wordt ingezet – het minste nadeel oplevert. Wanneer bijvoorbeeld de diensten de noodzakelijke gegevens kunnen verkrijgen door degene die toegang heeft tot de gegevens erom te vragen, zal voor dit middel worden gekozen. Dan kan en zal de inzet van een zwaardere bevoegdheid als het binnendringen in een geautomatiseerd werk achterwege blijven. Min of meer in het verlengde van het bepaalde in het eerste lid bepaalt artikel 26, vierde lid, dat een bevoegdheid onmiddellijk wordt gestaakt, indien het doel waartoe de bevoegdheid is uitgeoefend is bereikt dan wel met de uitoefening van een minder ingrijpende bevoegdheid kan worden volstaan. De proportionaliteitseis heeft zijn neerslag gekregen in artikel 26, tweede en derde lid: de uitoefening van een 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 bevoegdheden te maken inbreuk op de grondrechten van de burgers, in het bijzonder het recht op bescherming van de persoonlijke levenssfeer te legitimeren. Het is van groot belang dat deze afwegingen worden vastgelegd. Allereerst in de verzoeken om toestemming, zodat de met toestemmingverlening belaste instantie en voorts – voor zover er in een toets door de TIB is voorzien – de TIB deze in zijn beoordeling van het verzoek om toestemming onderscheidenlijk de verleende toestemming kan betrekken. Voorts is het vastleggen van de gemaakte afwegingen van belang in het kader van interne evaluaties alsmede het door de CTIVD uit te voeren rechtmatigheidstoezicht.

In de gevallen waarbij niet voorzien is in een wettelijk voorgeschreven toestemmingsregime, zal deze afweging dan dienen te blijken uit de ingevolge artikel 31 voorgeschreven aantekening die van de uitoefening van de bevoegdheid moet worden gemaakt.

3.3.2.3 Het onderzoek op relevantie van gegevens en de vernietiging van gegevens

In artikel 27 van het wetsvoorstel is de verplichting voor de diensten opgenomen om gegevens die zijn verkregen door uitoefening van een bijzondere bevoegdheid als

bedoeld in paragraaf 3.2.5 zo spoedig mogelijk op hun relevantie voor het onderzoek waarvoor ze zijn verworven te onderzoeken. Dit is een aanvulling op artikel 18 waarin is bepaald dat gegevens worden verwerkt voor een specifiek doel. Dat doel dient gelegen te zijn binnen de inlichtingen- of veiligheidstaken van de diensten en te worden vastgelegd in de motivering van het verzoek om toestemming. De ruwe opbrengst van de inzet van een bijzondere bevoegdheid mag alleen worden aangewend in het kader van het onderzoek waarbinnen de gegevens zijn verworven of ten behoeve van een ander lopend onderzoek dat onder de inlichtingen- of veiligheidstaken van de diensten valt. Gegevens waarvan is vastgesteld dat deze niet relevant zijn voor het onderzoek of een ander lopend onderzoek, dienen te worden vernietigd. Daarnaast wordt bepaald dat – voor zover bij de wet niet anders is bepaald – gegevens die nog niet op hun relevantie zijn onderzocht, na een jaar dienen te worden vernietigd. Deze termijn kan met ten hoogste zes maanden worden verlengd.

In het in internetconsultatie gegeven wetsvoorstel was de plicht tot onderzoek op relevantie slechts bij enkele bijzondere bevoegdheden opgenomen.[24] In de PIA Wiv (paragraaf 4.6.3) wordt geconstateerd dat de diensten alle gegevens die zij verzamelen binnen een redelijke termijn op hun relevantie beoordelen. Het verzamelen van gegevens is noodzakelijk voor het doen van onderzoek en indien het persoonsgegevens betreft moeten de daaraan verbonden privacyrisico's worden geminimaliseerd, waarbij het niet uitmaakt door middel van welke (bijzondere) bevoegdheid de gegevens zijn verkregen. Er is in het wetsvoorstel gekozen om deze onderzoeksplicht op relevantie in te voeren met betrekking tot gegevens die zijn verkregen met uitoefening van een bijzondere bevoegdheid als bedoeld in paragraaf 3.2.5. Gegevens verkregen door de uitoefening van andere bevoegdheden, zoals bijvoorbeeld het raadplegen van open bronnen of informanten, vallen buiten de werking van deze onderzoeksplicht. De achtergrond hiervan is dat het onderzoek van de diensten, net als bijvoorbeeld bij universiteiten en andere kennisinstituten, mede is gestoeld op langdurige dossieropbouw en studie op basis van niet-bijzondere bronnen. Zo verzamelen de diensten veel vakinhoudelijke informatie, aangaande onderwerpen als ontwikkelingen op het gebied telecommunicatie, biometrie, cryptografie, buitenlandse ontwikkelingen, demografie, terrorisme, wapensystemen, conflictgebieden, etc. Deze gegevens zijn jaren van belang voor de onderbouwing en duiding van informatie in onderzoeken, bijvoorbeeld bij het vervaardigen van normbeelden. Het gaat dan primair om open bronnen die voor een ieder toegankelijk zijn. Voorts vormen commerciële gegevens, (inter)nationale samenwerking (niet per se met diensten, maar ook met de NAVO, VN, EU,

[24] Te weten waar het gaat om gegevens verkregen door toepassing van de bijzondere bevoegdheid tot het binnendringen in een geautomatiseerde werk, gerichte interceptie, onderzoeksopdrachtgerichte interceptie en door het opvragen van opgeslagen gegevens bij een aanbieder van een communicatiedienst als onderdeel van die dienst.

krijgsmachten, onderzoekcentra etc.) en klassieke militaire sensoren niet-bijzondere bronnen. Een deel van de genoemde bronnen speelt tevens een rol bij veiligheidsonderzoeken, het opstellen van dreigings- en risicoanalyses en het bewaken en beveiligen van gegevens door de AIVD en MIVD. Dit betreffen taken van de diensten waarvoor geen bijzondere bevoegdheden kunnen worden ingezet. Langdurig terugkijken is niettemin nodig om ook deze taken goed en zorgvuldig te kunnen uitvoeren.

Het onderzoek op relevantie vindt plaats in het licht van het onderzoek waarvoor de gegevens zijn verzameld of ten behoeve van een ander lopend onderzoek als bedoeld in artikel 8, tweede lid, onder a en d, en de taken, bedoeld in artikel 10, tweede lid, onder a, c, en e. Is eenmaal de relevantie vastgesteld, dan kunnen deze gegevens worden bewaard en ook verder worden verwerkt, ook voor andere onderzoeken van de dienst waarvoor deze gegevens van belang kunnen zijn. Verwijdering en uiteindelijk vernietiging van deze gegevens is onderworpen aan het regime van artikel 20 van het wetsvoorstel.

De bewaartermijn waarvoor gegevens mogen worden onderzocht op relevantie is in onderhavig artikel voor alle bijzondere bevoegdheden, met uitzondering van één (te weten bij onderzoeksopdrachtgerichte interceptie ex artikel 48), gesteld op een jaar met de mogelijkheid deze eenmalig voor een periode van ten hoogste zes maanden te verlengen. Hiervoor kan onder omstandigheden aanleiding zijn, bijvoorbeeld indien de hoeveelheid verzamelde gegevens zodanig groot is dat deze redelijkerwijs bezien niet binnen de gestelde termijn kan worden bezien op relevantie. Maar ook bijvoorbeeld het ontbreken van voldoende vertaalcapaciteit kan onder omstandigheden reden zijn om tot verlenging over te gaan.

In artikel 27, tweede lid, is een specifieke bepaling opgenomen ter zake van gegevens die door de diensten zijn verzameld en betrekking hebben op de vertrouwelijke communicatie tussen een advocaat en diens cliënt in andere gevallen dan waarvoor op grond van artikel 30, derde lid, van het wetsvoorstel toestemming door de rechtbank Den Haag is verleend om *jegens een advocaat* bijzondere bevoegdheden in te zetten, waarbij de uitoefening kan leiden tot verwerving van gegevens die betrekking hebben op dergelijke vertrouwelijke communicatie. In laatstgenoemde situatie geldt gewoon de in artikel 27, eerste lid, van het wetsvoorstel neergelegde verplichting om zo spoedig mogelijk de relevantie te onderzoeken en niet-relevante gegevens te vernietigen. De in artikel 27, tweede lid, neergelegd regeling ziet echter op vertrouwelijke communicatie die *als bijvangst* bij de uitoefening van een bijzondere bevoegdheden die *jegens een ander* dan een advocaat wordt verkregen. Uitgangspunt daarbij is dat dergelijke gegevens terstond dienen te worden vernietigd, tenzij de verdere verwerking van de

desbetreffende gegevens noodzakelijk is voor het onderzoek in het kader waarvan ze initieel zijn verworven. Daarvoor is echter wel toestemming van de rechtbank Den Haag vereist; wordt deze toestemming niet verleend, dan dienen de gegevens alsnog terstond te worden vernietigd. Inherent aan dit stelsel is echter, dat de diensten dus wel al kennis kunnen nemen van de vertrouwelijke communicatie; er is dus niet voorzien in bijvoorbeeld een systeem van nummerherkenning, zoals dat wel in het kader van strafvordering wordt toegepast, waarbij gesprekken die worden gevoerd met bekend gestelde telefoonnummers van advocaten niet worden opgenomen. Nog los van het feit dat een systeem van nummerherkenning alleen toepasbaar is ingeval het gaat om het afluisteren van telefoon- of internetverkeer (in dat laatste geval wordt verkeer met een bepaald IP-adres niet opgenomen) en niet ingeval er door toepassing van andere bijzondere bevoegdheden (indirect) dergelijke vertrouwelijke communicatie beschikbaar kan komen (vgl. via een microfoon-actie bij een target thuis waarbij een gesprek met een advocaat wordt opgevangen), is het gelet op het door de diensten te behartigen belang van de nationale veiligheid onwenselijk om op voorhand communicatie als hier bedoeld – maar dat geldt evenzeer voor communicatie van journalisten –categorisch uit te sluiten van eventueel gebruik in onderzoeken van de diensten. Wel is het van belang dat een en ander met vergaande waarborgen is omgeven. Zo zal vertrouwelijke communicatie als hier bedoeld die niet van belang voor het onderzoek wordt geacht in het kader waarvan de gegevens zijn verworven (doelbinding) terstond dienen te worden vernietigd; bij een verzoek om toestemming aan de rechtbank voor verder gebruik zal men – in het licht van de eisen gesteld in artikel 18 van het wetsvoorstel – men de noodzaak voor het onderzoek dienen aan te tonen. Er geldt een zogenaamde verzwaarde proportionaliteitstoets; niet alleen dient bij de inzet van bijzondere bevoegdheden naast het belang van de bescherming van de persoonlijke levenssfeer in algemene zin, het bijzondere belang van de verschoningsgerechtigde meegewogen te worden maar tevens moet er sprake zijn van concrete aanwijzingen dat er een direct gevaar voor de nationale veiligheid is. Een vergelijkbare regeling (ook qua reikwijdte beperkt tot bijzondere bevoegdheden) is opgenomen in artikel 7 van de Tijdelijke regeling onafhankelijke toetsing bijzondere bevoegdheden Wiv 2002 jegens advocaten en journalisten[25], zij het dat daar – in afwachting van een formeelwettelijke regeling – de toets (bindend advies) is belegd bij de tijdelijke onafhankelijke toetsingscommissie bijzondere bevoegdheden Wiv 2002 jegens advocaten en journalisten. Deze regeling komt te vervallen indien onderhavig wetsvoorstel tot wet wordt verheven en in werking treedt.

3.3.2.4 Het toepassingsbereik van de bijzondere bevoegdheden

[25] Stcrt. 2015, 46477.

In artikel 28 van het wetsvoorstel is bepaald in welke gevallen door de diensten de in paragraaf 3.2.5 opgenomen bijzondere bevoegdheden mogen worden uitgeoefend. Daarmee is allereerst aangesloten bij de huidige regeling, zoals opgenomen in artikel 18 Wiv 2002 (zie artikel 28, 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 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 bevoegdheid tot het verzamelen van gegevens uit open bronnen, uit informatiebronnen waar de diensten een recht op kennisneming van de aldaar berustende gegevens is verleend, de raadpleging van informanten en in voorkomend gevallen via bevraging van informatie van buitenlandse collegadiensten. 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 dreigingsanalyses 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 in 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.[26] 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 28, tweede lid, wordt voor deze twee specifieke gevallen de uitoefening van bijzondere bevoegdheden mogelijk gemaakt.

Zo wordt in artikel 28, tweede lid, aanhef en onder a, bepaald dat een bevoegdheid als bedoeld in paragraaf 3.2.5 – 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 23, aanhef en onder c). Het kan daarbij zowel gaan om eigen medewerkers als om derden, zoals informanten en agenten. 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 (mogelijke) risico's die een informant of agent loopt noodzakelijk zijn om zicht te krijgen op de omgeving of het netwerk waarin deze zich begeeft, bijvoorbeeld door hem te volgen (contra-observatie) 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 28, tweede lid, onder b,

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

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. Maar ook kan het noodzakelijk zijn om de betrouwbaarheid van de bron te toetsen doordat er gerede twijfels zijn over het waarheidsgehalte van de verklaringen van de bron. De in artikel 28, tweede lid, voorziene mogelijkheden om ook ter ondersteuning van een goede taakuitvoering bijzondere bevoegdheden in te kunnen zetten, zijn echter wel onderworpen aan extra voorwaarden, in het bijzonder waar het gaat om het verlenen van toestemming.

Tot slot wordt erop gewezen dat in de PIA Wiv (paragraaf 4.4.1) wordt opgemerkt dat met deze uitbreiding van de inzet van bijzondere bevoegdheden ten behoeve van deze doeleinden geen grote privacyrisico's voordoen. Het doel van het onderzoek is specifiek afgebakend en gericht op de persoon zelf; voorts wordt een zorgvuldigheidsbelang gediend, dat ten goede komt aan de algemene kwaliteit van de werkzaamheden van de diensten en ook als zodanig een privacywaarborg dient.

3.3.2.5 Het toestemmingsregime voor bijzondere bevoegdheden

3.3.2.5.1 Algemeen

Anders dan in de huidige wet is bepaald, is – met uitzondering van de toestemmingverlening in bijzondere gevallen (artikel 30) – bij iedere bijzondere bevoegdheid aangegeven welke persoon of instantie bevoegd is toestemming te verlenen voor de uitoefening van de desbetreffende bijzondere bevoegdheid alsmede of en, zo ja, in hoeverre de mogelijkheid tot mandaat bestaat. Daarmee is uitvoering gegeven aan het advies (onderdeel 8) van Afdeling advisering van de Raad van State, waarin zij aangaf dat een algemene regeling in combinatie met een groot aantal afwijkende bepalingen in de artikelen die zien op specifieke bijzondere bevoegdheden resulteerde in een onoverzichtelijk beeld.

Niettegenstaande het voorgaande gelden waar het gaat om de bevoegdheid tot het verlenen van toestemming wel enkele uitgangspunten. De bevoegdheid om toestemming te verlenen is primair in handen van de voor de dienst verantwoordelijke minister gelegd, indien het gaat om de toepassing van bevoegdheden die al naar gelang de aard daarvan en de omstandigheden waarin deze worden toegepast, een ingrijpend 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 overigens niet dat de toestemmingverlening in alle gevallen door de betrokken minister persoonlijk dient plaats te vinden. Mandaat moet niettemin 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. Zoals eerder is aangegeven is bij de desbetreffende bijzondere bevoegdheden bepaald of en, zo ja, in hoeverre de mogelijkheid van mandaat (en ondermandaat) bestaat. De mogelijkheid van ondermandaat door het hoofd van de dienst is in de gevallen waarin dit is toegestaan, uitsluitend toegestaan aan hem ondergeschikte ambtenaren. Ondermandaat aan niet aan hem ondergeschikte ambtenaren, zoals bijvoorbeeld de ambtenaren als bedoeld in artikel 91 en 92, 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.[27]

De 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 29, eerste 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.[28] Dit komt eveneens overeen met de thans bestaande regeling (artikel 19, derde lid, Wiv 2002). In artikel 29, tweede lid, wordt bepaald aan welke eisen verzoeken om toestemming dienen te voldoen.

3.3.2.5.2 De inhoud van een verzoek om toestemming

[27] Vgl. de Mandaatregeling Defensie Wet op de inlichtingen- en veiligheidsdiensten 2002 en Wet veiligheidsdiensten (Stcrt. 2002, 147); de mandaatregeling van de minister van BZK met betrekking tot de AIVD is niet gepubliceerd.
[28] 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.

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 29, tweede 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. Naast hetgeen ingevolge artikel 29, tweede lid, in een verzoek dient te worden opgenomen, wordt bij enkele bijzondere bevoegdheden nog voorzien in de verplichting om – op de desbetreffende bijzondere bevoegdheid toegesneden - aanvullende informatie op te nemen, die van belang is bij de beoordeling van het verzoek om toestemming.

Het verzoek om toestemming dient allereerst aan te geven voor welke bijzondere bevoegdheid toestemming wordt gevraagd. Tevens dient – voor zover van toepassing – het verzoek gegevens te bevatten betreffende de identiteit van de persoon dan wel de organisatie ten aanzien van wie onderscheidenlijk waarvan de uitoefening van de desbetreffende bevoegdheid wordt verlangd. Voor zover de persoon werkzaam is als journalist of advocaat, dient in het verzoek om toestemming deze hoedanigheid te worden vermeld. 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.[29]

3.3.2.5.3 Toestemmingverlening in bijzondere gevallen

[29] 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.

In artikel 30 van het wetsvoorstel wordt voor een drietal bijzondere gevallen een van het reguliere, bij iedere bijzondere bevoegdheid, aangegeven toestemmingsregiem afwijkende regeling gegeven. Het gaat hierbij om de uitoefening van bijzondere bevoegdheden ter ondersteuning van een goede taakuitvoering en de uitoefening van bijzondere bevoegdheden jegens journalisten en advocaten in bepaalde gevallen.

Uitoefening van bijzondere bevoegdheden ter ondersteuning van een goede taakuitvoering

In artikel 30, eerste 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 28, tweede lid, van het wetsvoorstel thans voorziet. Allereerst is bepaald dat de toestemming in deze gevallen uitsluitend door de minister kan worden verleend op een daartoe strekkend 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 vier weken 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 29, tweede 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 28, eerste lid, afwijkende uitoefening van een bijzondere bevoegdheid, dient de CTIVD terstond op de hoogte te worden gesteld van een verleende toestemming (artikel 30, eerste lid, laatste volzin).

Uitoefening van bijzondere bevoegdheden jegens journalisten en advocaten in bepaalde gevallen

In artikel 30, tweede en derde lid, van het wetsvoorstel wordt voor een tweetal bijzondere situaties de bevoegdheid tot het verlenen van toestemming in handen gelegd van de rechtbank Den Haag.[30] Het betreft hier de uitoefening van bijzondere bevoegdheden jegens een journalist, waarbij de uitoefening van de bevoegdheid kan leiden tot verwerving van gegevens inzake de bron van de journalist, en de uitoefening van bijzondere bevoegdheden jegens een advocaat, waarbij de uitoefening kan leiden tot verwerving van gegevens die betrekking hebben op de vertrouwelijke communicatie tussen een advocaat en diens cliënt.

[30] Naast de onder de huidige Wiv 2002 reeds bestaande situatie, waarbij voor het openen van brieven en andere geadresseerde zendingen waarvoor eveneens in toestemmingverlening door de rechtbank Den Haag is voorzien.

Artikel 30, tweede lid, bepaalt dat de uitoefening van een bevoegdheid als bedoeld in paragraaf 3.2.5 *jegens een journalist, waarbij de uitoefening van de bevoegdheid kan leiden tot verwerving van gegevens inzake de bron van de journalist*, slechts is toegestaan, indien de rechtbank daartoe op verzoek van de betrokken minister, toestemming heeft verleend. Deze specifieke regeling, die naar aanleiding van het advies van de Afdeling advisering van de Raad van State overigens niet meer beperkt is tot de uitoefening van een bijzondere bevoegdheid jegens een journalist die *gericht* is op het achterhalen van een bron, 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 10 EVRM.[31] 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.[32] 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.[33] De bevoegdheid tot het verlenen van toestemming voor de uitoefening van de bevoegdheden als bedoeld in paragraaf 3.2.5, voor zover deze worden toegepast jegens journalisten en de toepassing kan leiden tot het achterhalen van hun bronnen, is in handen gelegd van de rechtbank Den Haag. Op deze wijze wordt tegemoet gekomen aan de door het EHRM geformuleerde eis dat er in onderhavige gevallen voorzien dient te zijn in een voorafgaande toets door een onafhankelijke instantie met de bevoegdheid de toepassing ervan te voorkomen. De keuze voor de rechtbank Den Haag is ingegeven door het feit dat deze reeds ervaring heeft met het verlenen van toestemming op grond van artikel 23 Wiv 2002 (openen van brieven en andere geadresseerde zendingen), er aldus wordt voorzien in één uniform regime. Daarnaast wordt er hiermee voor gezorgd dat de kennis omtrent operationele activiteiten van de beide diensten niet verder bekend raakt dan strikt noodzakelijk is. Een verzoek om toestemming dient te worden gedaan door de voor de desbetreffende dienst verantwoordelijke Minister. De reden om het verzoek aan de rechtbank te doen uitgaan van de Minister en dus niet in mandaat door het hoofd van de dienst is, dat, nu het hier gaat om inbreuk op het recht op journalistieke bronbescherming dat een hoge mate van bescherming geniet en inbreuken daarop slechts in uitzonderlijke gevallen gelegitimeerd zijn, de afweging ter zake op het

[31] EHRM 22 november 2012, *Telegraaf Media Nederland Landelijke Media B.V. en anderen t. Nederland*.
[32] Kamerstukken II 2012/13, 30 977, nr. 49.
[33] Kamerstukken II 2014/15, 34 027, nrs. 1-4.

hoogste niveau, te weten bij de voor de dienst verantwoordelijke minister, is aangewezen. Het in het wetsvoorstel neergelegde afwegingskader voor de uitoefening van bijzondere bevoegdheden is onverkort van toepassing. De eis van toestemming door de rechtbank geldt voor *alle* in paragraaf 3.2.5 geregelde bevoegdheden, ook in die gevallen waar ten aanzien van een specifieke bevoegdheid geen toestemming is vereist. In artikel 30, tweede lid, van het wetsvoorstel is voorts het voor de toepassing van de regeling essentiële begrip «bron» nader uitgewerkt. Onder bron in het kader van dit wetsvoorstel wordt verstaan: de persoon die gegevens ter openbaarmaking aan een journalist heeft verstrekt. Er is echter afgezien van een wettelijke definitie van het begrip «journalist». Aangesloten wordt bij de invulling die in het kader van de jurisprudentie van het EHRM daaraan wordt gegeven. Daarmee kan de invulling van het begrip en daarmee de reikwijdte van de voorgestelde regeling mee evolueren met de ontwikkeling in de jurisprudentie van het EHRM, een en ander bezien in het kader van de reikwijdte van deze wet en het optreden van de betrokken diensten.

Artikel 30, derde lid, bepaalt dat de uitoefening van een bevoegdheid als bedoeld in paragraaf 3.2.5 *jegens een advocaat, waarbij de uitoefening kan leiden tot de verwerving van gegevens die betrekking hebben op de vertrouwelijke communicatie tussen een advocaat en diens cliënt*, slechts is toegestaan, indien de rechtbank Den Haag daartoe, op een daartoe strekkend verzoek van de betrokken minister, toestemming heeft verleend. Deze regeling is opgenomen naar aanleiding van recente jurisprudentie (voorzieningenrechter rechtbank Den Haag, 1 juli 2015, en het gerechtshof Den Haag, 27 oktober 2015)[34], waarin is geoordeeld dat het door de AIVD en MIVD (direct en indirect) tappen, ontvangen, opnemen, afluisteren en uitwerken van elke vorm van communicatie (hierna: tappen) van en met advocaten in strijd is met artikel 8 EVRM, en dat het verboden is om aldus verkregen informatie, voor zover deze onder het verschoningsrecht van de advocaat valt, op grond van artikel 38 Wiv 2002 aan het openbaar ministerie te verstrekken omdat dit leidt tot een ernstige inbreuk op artikel 6, derde lid, onder c, EVRM. In het huidige wettelijke systeem is namelijk niet voorzien in de mogelijkheid van een voldoende onafhankelijk toezicht door een orgaan dat ten minste de bevoegdheid heeft het tappen te voorkomen of te beëindigen. Het huidige stelsel, waarbij de CTIVD achteraf de verleende toestemmingen voor het tappen van advocaten kan beoordelen op rechtmatigheid, wordt door de rechter onvoldoende geacht omdat de CTIVD de bevoegdheid ontbeert om het tappen te beëindigen. Bij brief van 27 juli 2015[35] heeft het kabinet aan de Tweede Kamer laten weten dat het grote waarde hecht aan het belang dat verdachten en andere procespartijen een eerlijk proces moeten

[34] ECLI:NL:RBDHA:2015:7436 en ECLI:NL:2015:2881.
[35] Kamerstukken II 2014/15, 29 279, nr. 268.

krijgen en dat zij in dit verband onbelemmerd toegang tot een advocaat moeten kunnen hebben. Daarbij heeft het kabinet aangegeven dat er voorzien zal worden in een vorm van onafhankelijke toetsing bij het tappen van advocaten, echter dat daarvoor wijziging van de wet noodzakelijk is. De in artikel 30, derde lid, opgenomen regeling strekt ter uitwerking daarvan. Daarbij is ervoor gekozen om aan te sluiten bij de voorgenomen regeling voor journalisten, dat wil zeggen dat de bevoegdheid voor het verlenen van toestemming in handen wordt gelegd van de rechtbank Den Haag en voorts dat die toestemming is vereist voor de uitoefening van *alle* bijzondere bevoegdheden (en dus niet alleen het tappen, zoals geregeld in artikel 47 van het wetsvoorstel) voor zover de uitoefening daarvan – in casu – kan leiden tot het verwerven van gegevens die betrekking hebben op de vertrouwelijke communicatie tussen een advocaat en diens cliënt. Waar het gaat om de verstrekking van dergelijke communicatie aan het openbaar ministerie (een ander element uit de uitspraak van de voorzieningenrechter) is daarvoor in artikel 66, derde lid, van het wetsvoorstel een voorziening getroffen; kortheidshalve wordt naar de toelichting ter zake verwezen. Evenals bij de regeling voor journalisten is de maximale toestemmingstermijn (regulier ten hoogste drie maanden) beperkt tot ten hoogste vier weken en kan telkens op een daartoe strekkend verzoek worden verlengd voor eenzelfde periode. Het verzoek dient te voldoen aan de vereisten van artikel 29, tweede lid; voorts geldt hierbij – evenals bij de journalisten – een verzwaarde proportionaliteitstoets; niet alleen dient bij de inzet van bijzondere bevoegdheden naast het belang van de bescherming van de persoonlijke levenssfeer in algemene zin, het bijzondere belang van de verschoningsgerechtigde meegewogen te worden maar tevens moet er sprake zijn van concrete aanwijzingen dat er een direct gevaar voor de nationale veiligheid is.

3.3.2.5.4 De verslaglegging inzake de uitoefening van bevoegdheden tot verzamelen van gegevens

In artikel 33 Wiv 2002 is thans bepaald dat van de uitoefening van een bijzondere bevoegdheid een schriftelijk verslag wordt gemaakt. Daaraan zijn geen andere eisen gesteld dan dat het verslag schriftelijk dient te zijn; voor het overige kan de wijze van verslaglegging plaatsvindt – al naar gelang de bijzondere bevoegdheid die het betreft - op een flexibele manier worden ingevuld. Deze verslaglegging is niet alleen van belang voor interne controledoeleinden, maar ook om een effectief toezicht door de CTIVD mogelijk te maken. Voorts kan het verslag een rol spelen bij het uit te brengen notificatieverslag, dat in artikel 59 ten aanzien van een aantal bijzondere bevoegdheden is voorgeschreven. In artikel 31 van het wetsvoorstel komt deze plicht tot verslaglegging in aangepaste vorm terug. Allereerst is de reikwijdte van de verslagplicht uitgebreid tot alle bevoegdheden die worden ingezet voor het verzamelen van gegevens. Voorts is de

formulering van de verplichting aangepast, zodat ook andere vormen dan schriftelijke verslaglegging zijn toegestaan; een voorbeeld daarvan vormt geautomatiseerde verslaglegging (zoals logging). Vanuit het oogpunt van beheersbaarheid van de administratieve lasten dient het gebruik van (traditionele) media en openbare publicaties hiervan te zijn uitgezonderd. Zelfs geautomatiseerde verslaglegging hiervan zou een belasting opleveren die in geen verhouding staat tot de veronderstelde waarborgfunctie.

3.3.3 De Toetsingscommissie inzet bevoegdheden

3.3.3.1 Algemeen

In paragraaf 3.2.2 wordt voorzien in een nieuwe commissie, te weten de Toetsingscommissie inzet bevoegdheden (TIB). Deze onafhankelijke commissie krijgt die tot taak om de verleende toestemming voor enkele bijzondere bevoegdheden op rechtmatigheid te toetsen; indien deze toets tot het oordeel leidt dat de toestemming niet rechtmatig is verleend, dan vervalt de toestemming van rechtswege en mag de bevoegdheid niet worden uitgeoefend.

De introductie van deze nieuwe commissie vindt plaats naar aanleiding van het feit dat velen in het kader van de internetconsultatie hebben betoogd dat de modernisering van de bijzondere bevoegdheden gepaard zou moeten gaan met de introductie van een onafhankelijke (rechterlijke) toets voordat tot de uitoefening van deze bevoegdheden wordt overgegaan. Dit is ook één van de conclusies in de studie 'Het mensenrechtenkader voor het Nederlandse stelsel van toezicht op de inlichtingen- en veiligheidsdiensten' van de Afdeling staats- en bestuursrecht van de Universiteit Leiden. De CTIVD voegde deze studie als bijlage bij haar reactie op het wetsvoorstel in de internetconsultatie.[36]

De regering heeft zich uitgebreid beraad op de wenselijkheid van de introductie van een dergelijke toets. Bij dit beraad hebben twee zaken een doorslaggevende rol gespeeld.

Ten eerste is met de jurisprudentie van het Europees Hof ter bescherming van de Rechten van de Mens (EHRM) een koers ingezet die gaat richting een voorkeur voor een dergelijke toets. Bovendien staat het een lidstaat bij het EVRM vrij om strengere eisen te stellen aan beperking van de daarin gegarandeerde mensenrechten dan strikt genomen uit het EVRM en de jurisprudentie van het EHRM voortvloeien.

Ten tweede acht de regering, zoals eerder gesteld, een snelle inwerkingtreding van de mogelijkheid tot onderzoeksopdrachtgerichte interceptie noodzakelijk, maar heeft zij ook zeker begrip voor de maatschappelijke zorgen voor de inbreuk op de persoonlijke

[36] http://www.ctivd.nl/documenten/publicaties/2015/08/26/rapport-universiteit-leiden.

levenssfeer die hiermee gepaard kan gaan. Zij wil graag tegemoetkomen aan deze zorg. Door de inzet van de bevoegdheden die in potentie kunnen leiden tot de zwaarste inbreuk op de persoonlijke levenssfeer niet toe te staan dan nadat een onafhankelijke instantie hiermee heeft ingestemd wordt voorzien in een stevige waarborg.

De regering heeft aldus besloten om voordat wordt overgegaan tot de inzet van die bijzondere bevoegdheden die een zware inbreuk kunnen maken op de persoonlijke levenssfeer een voorafgaande, onafhankelijke, bindende toets in te voeren. Deze toets zal worden uitgevoerd door de nieuwe onafhankelijke Toetsingscommissie Inzet Bevoegdheden (TIB). De TIB zal bestaan uit drie personen, waarvan tenminste twee personen een achtergrond als rechter dienen te hebben; als derde lid kan een persoon worden benoemd, die bijvoorbeeld over technische deskundigheid en inzicht in veiligheidsrisico's beschikt. Daarmee wordt tegemoet gekomen aan de kritiek van de Afdeling advisering van de Raad van State dat het bij de beoordeling van de noodzaak en proportionaliteit van de inzet van grootschalige interceptie van belang is dat de TIB ook over deze deskundigheid beschikt. De regering kiest voor een gespecialiseerde commissie, waarin kennis en expertise worden gebundeld.

Ten eerste heeft een substantieel deel van de inzet van bijzondere bevoegdheden door de inlichtingen- en veiligheidsdiensten betrekking op het buitenland en de persoonlijke levenssfeer van niet-Nederlanders. Een Nederlandse rechter zal zich niet bevoegd achten zich over deze inbreuk uit te spreken, omdat deze zich strikt genomen niet beperkt tot de Nederlandse jurisdictie. Overigens is deze problematiek internationaal bekend. Veel landen maken daarom onderscheid in inzet van bijzondere bevoegdheden betreffende de eigen jurisdictie enerzijds en het buitenland anderzijds. Betreffende de inzet betreffende het buitenland is dan in voorkomend geval voorzien in een speciale commissie, maar niet in een rechterlijke toets. In Nederland is evenwel al in 2002 gekozen om geen onderscheid te maken in een inlichtingen- en veiligheidsdienst voor het binnenland en één voor het buitenland. Deze keus is nog steeds de enige juiste gelet op het huidige dreigingsbeeld, waarin dreiging vanuit het buitenland zich razendsnel kan ontwikkelen tot een dreiging voor Nederland.

Ten tweede betreft de uit te voeren toets een specialistische toets op rechtmatigheid (inclusief noodzaak, proportionaliteit en subsidiariteit), waarbij de belangen dienen te worden gewogen van de nationale veiligheid en de persoonlijke levenssfeer. Additionele kennis en kunde van het werk en de praktijk van de inlichtingen- en veiligheidsdiensten is hiervoor vereist. Ook dit pleit voor de introductie van een aparte, gespecialiseerde commissie met tenminste twee deskundige juristen met een rechterlijke achtergrond

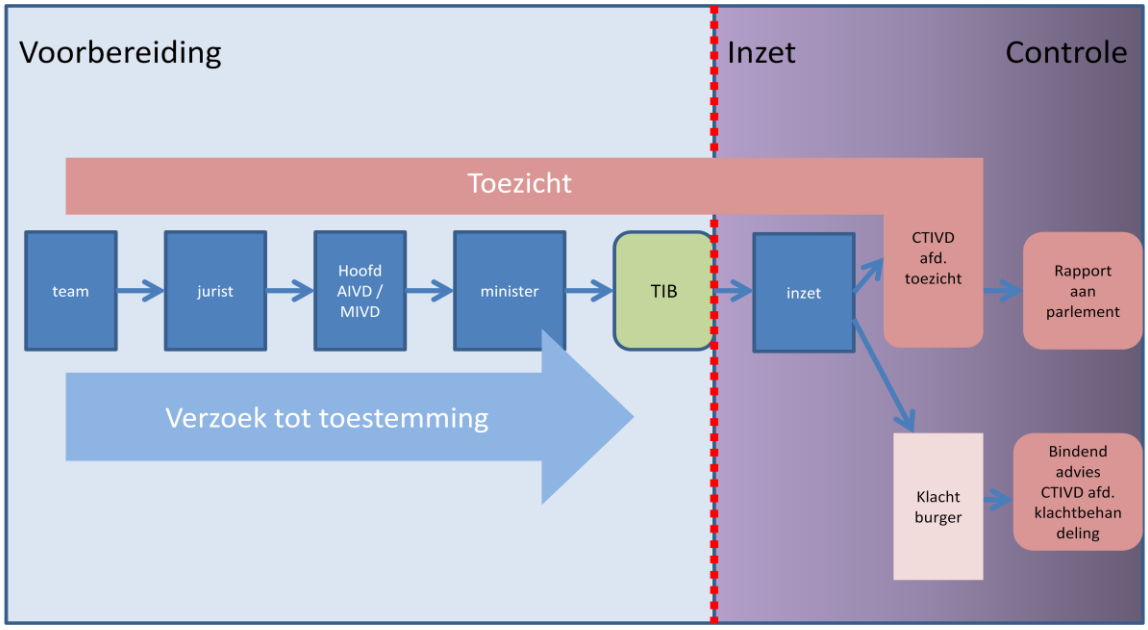
(ervaren juristen die minimaal zes jaar de functie van rechter hebben bekleed). Zij zullen gedurende langere tijd zitting in de TIB kunnen nemen en expertise kunnen opbouwen.

Voor de inzet van bevoegdheden jegens advocaten en journalisten met het oog op de relatie met hun cliënten respectievelijk bronnen is overigens wel voorzien in een voorafgaande rechterlijke toets (artikel 30). Daarbij moet worden opgemerkt dat de bedoelde inzet jegens advocaten en journalisten zelden voorkomt. De uitoefening van bevoegdheden jegens journalisten met het oog op hun relatie met bronnen wordt restrictief toegepast.

De TIB zal geheel los staan van de CTIVD. De CTIVD houdt toezicht achteraf op de rechtmatige uitvoering van de wet en behandelt klachten hierover, terwijl de TIB een bindende toets uitvoert voorafgaand aan de inzet van bepaalde bijzondere bevoegdheden. Nu de toets op de rechtmatigheid van het door de minister genomen besluit voorafgaand aan de inzet van een bijzondere bevoegdheid exclusief bij de TIB is belegd, brengt dat met zich mee dat de CTIVD de rechtmatigheid van dat besluit in beginsel dient te respecteren; slechts indien de CTIVD in het kader van haar toezicht op de uitvoering van een dergelijk besluit constateert dat het door de minister genomen besluit en ter toetsing aan de TIB voorgelegde besluit is gebaseerd op onvolledige of onjuiste informatie, kan zij dit als bevinding aan de minister rapporteren. De minister zal dan dienen te bezien of er aanleiding is een nieuw besluit te nemen en dat (opnieuw) aan de TIB voor te leggen. Het voorgaande is mutatis mutandis van toepassing indien het gaat om een toestemming die door de rechtbank Den Haag is verleend.

Vanuit het oogpunt van het vermijden van de (schijn van) partijdigheid of vooringenomenheid is het van belang dat de toetsing vooraf en het toezicht tijdens en achteraf bij verschillende instanties zijn belegd. De enige uitzondering op deze scheiding betreft de opleiding van de leden en het secretariaat van de TIB, die vanwege het specifieke werkveld en de bijzondere expertise zal worden vormgegeven in nauw overleg met de CTIVD.

Hiermee komt het toezichtssysteem er als volgt uit te zien:



3.3.3.2 De instelling, taakstelling en samenstelling van de TIB

Artikel 32 van het wetsvoorstel regelt de instelling en taakstelling van de TIB. Artikel 33 de samenstelling. De TIB bestaat uit drie leden. Tenminste twee van de drie leden dienen ten minste zes jaren de functie van rechterlijk ambtenaar met rechtspraak belast als bedoeld in artikel 1, onderdeel c, van de Wet op de rechterlijke organisatie, te hebben vervuld. Dat betekent dat de commissie in ieder geval zal worden bemenst met twee ervaren rechters. Het derde te benoemen lid kan, maar hoeft niet per se ook een rechter te zijn; dat biedt de mogelijkheid om een lid met andersoortige kennis en expertise in de commissie te benoemen (zie ook hetgeen in paragraaf 3.3.3.1 is gesteld). De leden worden benoemd voor een periode van zes jaren en kunnen eenmaal worden herbenoemd. Tevens zijn dezelfde bepalingen over onder meer schorsing, ontslag en incompatibiliteiten van toepassing als die gelden voor de leden van de CTIVD. Leden van de TIB zijn niet tevens lid van de CTIVD of de afdeling klachtbehandeling van de CTIVD. Een secretariaat zal de leden ondersteunen. De functies van de leden van de TIB alsmede de functies bij het secretariaat zullen op grond van artikel 3 van de Wet veiligheidsonderzoeken als vertrouwensfuncties worden aangewezen.

De leden van de TIB zullen op dezelfde manier worden benoemd als de leden van de CTIVD (artikel 33, vierde lid, van het wetsvoorstel verklaart daartoe artikel 99 – grotendeels – van overeenkomstige toepassing). Deze procedure draagt, naast diverse wettelijke waarborgen, bij aan de onafhankelijke positie van de TIB.

3.3.3.3 De toetsing door de TIB

De TIB is ingevolge artikel 32, tweede lid, belast met het toetsen van de rechtmatigheid van de door de betrokken minister verleende toestemming als bedoeld in de aldaar genoemde artikelen. Het gaat daarbij om de toestemming voor de volgende bijzondere bevoegdheden:

- De toepassing van observatie- en registratiemiddelen binnen woningen (artikel 40, derde lid);
- Het onderzoek van besloten plaatsen, van gesloten voorwerpen en aan voorwerpen gericht op de vaststelling van de identiteit, voor zover het woningen betreft (artikel 42, vierde lid);
- Het verrichten van DNA-onderzoek (artikel 43, tweede en vierde lid);
- Het verkennen van en binnendringen in geautomatiseerde werken (artikel 45, derde, vijfde en tiende lid);
- Onderzoek van communicatie met betrekking tot specifieke personen, organisaties en nummers, waaronder de telefoontap valt (artikel 47, tweede lid);
- Elk van de drie stappen in het onderzoeksopdrachtgerichte interceptieproces: de onderzoeksopdrachtgerichte interceptie, de selectie van de opbrengst alsmede de geautomatiseerde data-analyse, voor zover gericht op het identificeren van personen of organisaties (artikel 48, tweede lid, 49, vierde lid en 50, tweede en vierde lid);
- Het opdracht geven aan een aanbieder van een communicatiedienst – niet zijnde een aanbieder van een openbaar telecommunicatienetwerk of openbare telecommunicatiedienst - om medewerking te verlenen aan de uitvoering van een opdracht tot gerichte of onderzoeksopdrachtgerichte interceptie (artikel 53, tweede lid);
- Het opdracht geven aan een aanbieder van een communicatiedienst in verband met door hem als onderdeel van de door hem verleende communicatiedienst opgeslagen gegevens van een gebruiker dan wel aan een persoon of instantie die in het kader van de uitoefening van een beroep of bedrijf de opslag verzorgt van door derden via geautomatiseerde werken verwerkte gegevens, om de door hen opgeslagen in dit kader gegevens te verstrekken (artikel 54, tweede lid);
- Het opdracht geven om medewerking te verlenen bij de ontsleuteling van communicatie (decryptie) (artikel 57, tweede lid).

Het betreft de bevoegdheden die worden aangemerkt als in potentie het meest inbreuk makend op de persoonlijke levenssfeer en waarvoor ministeriële toestemming is benodigd. Het betreft die bevoegdheden waarvoor in het in consultatie gegeven wetsvoorstel voorzien was in de zogeheten heroverwegingsverplichting voor de minister.

Een door de minister verleende toestemming dient door hem op grond van artikel 36, eerste lid, te worden voorgelegd aan de TIB. Daarbij verstrekt hij de toetsingscommissie het aan de toestemming ten grondslag liggende verzoek om toestemming en diens besluit; indien de TIB naar aanleiding daarvan het noodzakelijk acht de beschikking te krijgen over aanvullende informatie, zijn de ministers verplicht om die aan de TIB te verstrekken. Anders dan de CTIVD heeft de TIB geen rechtstreekse toegang tot de gegevens bij de AIVD en de MIVD; dat is ook niet nodig nu de taak van de TIB zich – anders de CTIVD– beperkt tot een rechtmatigheidstoets op een voorgelegd verzoek. Bij de rechtmatigheidstoets door de TIB wordt beoordeeld of de verleende toestemming voldoet aan de eisen van noodzakelijkheid, proportionaliteit en subsidiariteit. De toetsing van de door de minister verleende toestemmingen door de TIB is in die zin vergelijkbaar met de toets die door de rechtbank Den Haag wordt verricht bij verzoeken ex artikel 23 Wiv 2002 (openen van brieven). De TIB dient zo spoedig mogelijk omtrent een voorgelegde toestemming te oordelen. De commissie kan de voorbereiding van het oordeel over een ter toetsing voorgelegd besluit toedelen aan een lid van de TIB; het is echter de commissie die uiteindelijk het oordeel vaststelt. Het oordeel van de TIB is bindend.

De feitelijke uitoefening van een bijzondere bevoegdheid kan, behoudens spoedgevallen, pas aanvangen nadat de TIB heeft geoordeeld dat de toestemming door de minister rechtmatig is verleend (artikel 36, tweede lid). In het geval dat de TIB een verleende toestemming onrechtmatig acht, dient zij haar oordeel met redenen omkleed aan de betrokken minister mede te delen en komt de toestemming van rechtswege te vervallen. De betrokken minister staat het vervolgens vrij om – rekening houdend met de redenen waarop een negatief oordeel van de TIB is gebaseerd – wederom toestemming te verlenen, waarna deze voor een nieuwe toets aan de TIB dient te worden voorgelegd.

In artikel 37 is voorzien in een procedure voor spoedgevallen. Deze houdt in dat indien onverwijlde spoed toepassing van de reguliere procedure niet toelaat, er reeds direct na het verlenen van de toestemming door de minister tot de uitoefening van de bevoegdheid kan worden overgegaan. In dat geval dient de minister de verleende toestemming onverwijld aan de TIB voor te leggen. Daarbij dient de TIB geïnformeerd te worden over de toepassing van de spoedprocedure alsmede de daaraan ten grondslag liggende redenen. De TIB dient de toepassing van de spoedprocedure mee te nemen in haar beoordeling. Ingeval de TIB de verleende toestemming onrechtmatig acht, vervalt de toestemming van rechtswege en dienen alle met de uitoefening van de desbetreffende bevoegdheid verzamelde gegevens terstond te worden vernietigd. Aangezien de TIB ook over de gevolgde spoedprocedure dient te oordelen, kan de situatie zich voordoen dat de TIB de verleende toestemming op zich rechtmatig acht

maar dat voor de toepassing van de spoedprocedure geen aanleiding ziet. Indien de TIB van oordeel is dat de spoedprocedure ten onrechte is gebruikt, maar de uitoefening van de bevoegdheid niettemin rechtmatig wordt geacht, bepaalt de TIB wat dient te gebeuren met de gegevens die eventueel zijn verkregen voordat de TIB zich heeft uitgesproken over de inzet.

In het door de TIB uit te brengen jaarverslag dient zij verantwoording afleggen over de wijze waarop zij haar werkzaamheden heeft verricht. Daarbij is aangesloten bij de regeling die voor de CTIVD geldt (artikel 35, derde lid, verklaart daartoe artikel 132 van overeenkomstige toepassing).

3.3.4 De bevoegdheden inzake de verzameling van gegevens

3.3.4.1 Algemeen

In artikel 25 van het wetsvoorstel worden de bevoegdheden geformuleerd die de diensten toekomen bij het verzamelen van gegevens. Een aantal bevoegdheden worden in het wetsvoorstel nader genormeerd. Het gaat daarbij om de bevoegdheid tot het stelselmatig verzamelen van gegevens omtrent personen uit open bronnen, de raadpleging van informanten en de bijzondere bevoegdheden. De eerste twee bevoegdheden zijn – evenals nu reeds het geval is –bij de uitvoering van alle taken van de diensten toepasbaar. De bijzondere bevoegdheden echter uitsluitend in de in artikel 28, eerste en tweede lid, van het wetsvoorstel genoemde gevallen.

3.3.4.2 Het stelselmatig verzamelen van gegevens over personen uit open bronnen

Over het algemeen zal het verzamelen van persoonsgegevens uit open bronnen (zoals kranten, tijdschriften, (het openbare deel van het) internet) niet tot een noemenswaardige inbreuk op iemands privacy leiden, maar dat wordt anders voor zover dit op een stelselmatige wijze plaatsvindt. In de PIA Wiv (par. 5.2) wordt daarvoor terecht aandacht gevraagd. Daarbij wordt ook verwezen naar de uitspraken van het EHRM in de zaken Rotaru t. Roemenië[37] en Association "21 Decembre 1989" e.a. t. Roemenië[38] ("*public information can fall within the scope of private life where it is systematically collected and stored in files held by the authorities*"). Dat brengt met zich mee dat een dergelijke vorm van gegevensverzameling moet voldoen aan de eisen van artikel 8, tweede lid, EVRM. In artikel 25, eerste lid, is reeds in algemene zin de bevoegdheid toegekend om gegevens te verzamelen uit voor een ieder toegankelijke informatiebronnen, zoals (het openbare deel van) internet. Daarmee wordt tegemoet gekomen aan de in de PIA Wiv (paragraaf 5.2.2) geuite wens om vanuit een oogpunt

[37] EHRM 4 mei 2000, *Rotaru t. Roemenië*, par. 43.
[38] EHRM 25 mei 2011, *Association "21 Decembre 1989" e.a. t. Roemenië*, par. 168.

van kenbaarheid een specifieke regeling te treffen voor OSINT (open bronnen informatie), omdat dit veel duidelijker voor de burgers is dan een impliciete bevoegdheid in te lezen in de algemene taakstelling van de diensten in de artikel 8 en 10 van het wetsvoorstel. Tevens wordt aldus uitdrukkelijk – naast de normen die aan gegevensverwerking als zodanig worden gesteld – aan deze vorm van gegevensverzameling de in artikel 26 geëxpliciteerde eisen van proportionaliteit en subsidiariteit van toepassing verklaard. De PIA Wiv gaat echter verder waar het gaat om het stelselmatig vastleggen van gegevens uit open bronnen en wel in de vorm van een bijzondere bevoegdheid die aan het algemene normeringskader voor bijzondere bevoegdheden is onderworpen. Alles afwegende zijn we tot de conclusie gekomen dat het aanmerken van deze bevoegdheid als een bijzondere bevoegdheid met alle gevolgen van dien niet wenselijk is. Met name het feit dat de toepassing van deze bevoegdheid buiten de gevallen als bedoeld in artikel 28 dan niet meer mogelijk zou zijn, speelt daarbij een doorslaggevende rol. Ook in het kader van bijvoorbeeld een veiligheidsonderzoek moet het mogelijk zijn en blijven dat omtrent een kandidaat-vertrouwensfunctionaris op een stelselmatige wijze gegevens uit open bronnen wordt verzameld; niet alleen eenmalig, maar op regelmatige basis gedurende de duur van het veiligheidsonderzoek. Het doel van een dergelijk onderzoek is immers juist erop gericht om een zo volledig mogelijk beeld van een persoon te krijgen (wat het doel van stelselmatig onderzoek is) om mede aan de hand daarvan te kunnen beoordelen of er geen risico's bestaan vanuit het oogpunt van de nationale veiligheid om betrokkene op een vertrouwensfunctie te doen benoemen. Nu echter belangrijke onderdelen van het normeringskader voor bijzondere bevoegdheden, met name de voorgeschreven toets aan proportionaliteit en subsidiariteit alsmede de plicht om van de uitoefening van de bevoegdheid aantekening te houden, in algemene zin van toepassing zijn op alle vormen van verzamelen van gegevens, en we tegelijkertijd erkennen dat vanuit een oogpunt van kenbaarheid en voorzienbaarheid een nadrukkelijke regeling van de bevoegdheid tot stelselmatig verzamelen van gegevens uit open bronnen wenselijk is, is in artikel 38 van het wetsvoorstel daartoe een regeling opgenomen. Voorts is vanwege het stelselmatige karakter van deze bevoegdheid en de implicaties die dat heeft voor de privacy van de betrokken persoon in artikel 38, tweede lid, van het wetsvoorstel bepaald dat de uitoefening van deze bevoegdheid slechts is toegestaan met toestemming van de voor de dienst verantwoordelijke minister of namens deze het hoofd van de dienst (met de mogelijkheid van ondermandaat).

3.3.4.3 De raadpleging van informanten

Artikel 39 van het wetsvoorstel regelt evenals het huidige artikel 17 Wiv 2002 de 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 allereerst onderworpen aan de algemene bepalingen inzake gegevensverwerking, zoals hiervoor reeds besproken. Dat betekent dus onder meer 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. Daarnaast zijn op de uitoefening van de bevoegdheid ook enkele algemene bepalingen inzake de verzameling van gegevens in paragraaf 3.2.1 van het wetsvoorstel van toepassing: het in artikel 26 neergelegde afwegingskader alsmede de in artikel 31 geregelde verplichting om van de uitoefening van de bevoegdheid aantekening te houden.

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 39, vijfde lid.

Artikel 17, derde lid, Wiv 2002 – en daarmee ook het voorgestelde artikel 39, vijfde 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.[39] 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 één 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 de Autoriteit Persoonsgegevens (AP)– in het kader van diens controlerende taak informatie te verstrekken over eventuele gegevensverstrekkingen aan de diensten, buiten toepassing blijft. Dat betekent niet dat er in het 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 39, 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 39, vijfde lid, neergelegde voorziening van toepassing is.

Ten opzichte van de huidige wettelijke regeling voorziet artikel 39 in een aantal aanvullingen. Allereerst wordt in artikel 39, derde lid, bepaald dat aan een verzoek om gegevensverstrekking kan worden voldaan door het verlenen van rechtstreeks

[39] 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 expliciete mogelijkheid wordt benoemd. Vergelijk onder meer de Wet politiegegevens, de Wet basisregistratie personen, de Wet justitiële en strafvorderlijke gegevens. In het kader van onderhavig wetsvoorstel is dan sprake van verzamelen van gegevens uit informatiebronnen waarvoor aan de dienst een recht op kennisneming van de aldaar berustende gegevens is verleend.

geautomatiseerde toegang tot de desbetreffende gegevens dan wel door het verstrekken van geautomatiseerde gegevensbestanden. Artikel 17 Wiv 2002 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, waarbij tegelijkertijd voor de situatie dat er rechtsreeks geautomatiseerde toegang wordt verleend nader wordt uitgewerkt op welke wijze deze wordt ingevuld (artikel 39, vierde lid, van het wetsvoorstel). 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 39 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. In artikel 39, vierde lid, van het wetsvoorstel is op een grotendeels vergelijkbare wijze als in artikel 24 Wet politiegegevens uitgewerkt op welke wijze de raadpleging van gegevens waartoe rechtstreeks geautomatiseerde toegang is verleend, kan plaatsvinden. Bij een dergelijke raadpleging vindt – zoals hiervoor reeds aangegeven – een zelfstandige bevraging, dat wil zeggen zonder verdere menselijke tussenkomst, van de gegevens plaats. Het gaat hier om een raadpleging op hit/no hit basis: door de diensten ingevoerde gegevens worden vergeleken met de gegevens bij de desbetreffende verantwoordelijke voor de gegevensverwerking. Is er sprake van een hit dan *kunnen* de daaraan gerelateerde gegevens aan de diensten worden verstrekt; het bestaan van een rechtstreeks geautomatiseerde toegang brengt immers geen plicht tot verstrekking met zich mee en de verantwoordelijke kan derhalve altijd een verstrekking tegenhouden. Er is voorts voorzien in nadere regelstelling bij of krachtens algemene maatregel van bestuur waar het gaat om de treffen technische en organisatorische maatregelen inzake rechtsreeks geautomatiseerde toegang. Dat ziet onder meer op maatregelen die aan de zijde van de verantwoordelijke voor de gegevensverwerking dienen te worden getroffen om met name de vertrouwelijkheid van de bevragingen door de diensten te waarborgen; de door de diensten ingevoerde gegevens zullen over het algemeen een staatsgeheim karakter dragen en daarvoor dienen – overigens mede met inachtneming van hetgeen voortvloeit uit het Besluit Voorschrift Informatiebeveiliging Rijksdienst Bijzondere Informatie 2013

(VIRBI 2013) – nadere regels te worden gesteld hoe deze aan de kant van de verantwoordelijke dienen te worden beveiligd.[40]

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 60 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 39, zesde 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 41, negende 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 concreet invulling gegeven aan een aspect van de in artikel 23 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 worden 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

[40] Zie bijvoorbeeld het Besluit beveiliging gegevens aftappen telecommunicatie, dat vergelijkbare regels stelt in het kader van bevragingen bij aanbieders van openbare telecommunicatienetwerken en –diensten.

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.

3.3.4.4 De bijzondere bevoegdheden tot verzameling van gegevens door de diensten

3.3.4.4.1 Algemeen

Naast algemene bevoegdheden van de diensten om gegevens te verzamelen en die voor alle taakonderdelen van de diensten kunnen worden ingezet, beschikken de AIVD en de MIVD ook over een aantal bijzondere bevoegdheden. Zoals in paragraaf 3.3.2.4 is toegelicht kunnen deze bevoegdheden slechts worden ingezet in de gevallen als bedoeld in artikel 28 van het wetsvoorstel. Het zijn over het algemeen bevoegdheden die – anders dan de algemene bevoegdheden tot gegevensverzameling – een meer ingrijpend karakter hebben en leiden tot een zwaardere inbreuk op het door artikel 8 EVRM gegarandeerde recht op privacy. Dat, zoals in het kader van de parlementaire behandeling van de huidige wet is gesteld, het bijzondere mede bepaald zou worden door het feit dat geheim dient te blijven in welke situatie jegens welke persoon of organisatie welke bevoegdheid wordt of is uitgeoefend[41], geldt onder omstandigheden evenzeer voor de uitoefening van de andere bevoegdheden tot gegevensverzameling, zoals de raadpleging van informanten. In die zin kan dat niet zozeer als het onderscheidende criterium worden beschouwd. Vanuit het perspectief van het EVRM is immers in beginsel bepalend de aard en mate waarop inbreuk wordt gemaakt op een daarin gegarandeerd mensenrecht, in het bijzonder het recht op privacy als bedoeld in artikel 8 EVRM. Zo wordt bijvoorbeeld interceptie van telecommunicatie[42] en onderzoek

[41] Kamerstukken II 1997/98, 25 877, nr. 3, blz. 24.
[42] EHRM 29 juni 2006, *Weber and Saravia t. Duitsland*.

van lichaamsmateriaal[43] als een zware inbreuk beschouwd die aan navenant zware eisen moet voldoen. Andere methodieken, zoals bijvoorbeeld het volgen van iemand met gebruikmaking van GPS-apparatuur, wordt daarentegen als minder inbreukmakend beschouwd.[44] Het ingrijpende 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 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

[43] EHRM 4 november 2008, *S. en Marper t. verenigd Koninkrijk*.
[44] EHRM 2 september 2010, *Uzun t. Duitsland*.

zwaarste inbreuken op het door artikel 8 EVRM gegarandeerde recht op privacy.[45] 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 28 jo. artikel 19 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 paragraaf 3.2.5 van het wetsvoorstel (in het bijzonder de subparagrafen 3.2.5.1 tot en met 3.2.5.7) 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.[46] 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 observeren en volgen (artikel 40) en het openen van brieven en andere geadresseerde zendingen (artikel 44). Met betrekking tot een enkele bestaande bijzondere bevoegdheid is een thans daarin besloten liggend aspect als een zelfstandige bijzondere bevoegdheid geformuleerd

[45] EHRM 29 juni 2006, *Weber and Saravia t. 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.

[46] Zie ook artikel 90, vijfde lid, van het wetsvoorstel, waar het gaat om het doen van verzoeken van ondersteuning door de AIVD en de MIVD *aan* buitenlandse collegadiensten waar het gaat om de uitoefening van bijzondere bevoegdheden (of handelingen die daarop zijn terug te herleiden).

(regeling DNA-onderzoek gericht op vaststelling, waaronder begrepen de verificatie, van een identiteit; artikel 43). 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 45). 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 3.2.5.6; de artikelen 46 tot en met 57). 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. Daarnaast hebben de reacties uit de internetconsultatie op een enkel onderdeel geleid tot aanpassing ten opzichte van het in internetconsultatie gegeven wetsvoorstel; dat betreft in het bijzonder de vergoeding van kosten. 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 58). In het onderstaande zullen de diverse bevoegdheden afzonderlijk worden toegelicht.

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 87 te vervallen. Voor de overwegingen daarvoor wordt kortheidshalve verwezen naar paragraaf 6.2 van deze toelichting.

3.3.4.4.2 Observeren en volgen

Artikel 40 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 40, 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; traditioneel wordt daarbij gedacht aan een verrekijker, foto- en video-apparatuur, maar door allerlei technologische ontwikkelingen komen in toenemende mate ook andere middelen beschikbaar. In de PIA Wiv (pag. 103) wordt daar op gewezen. Zo kunnen voor observatie- en volgdoeleinden ook *drones* worden ingezet, kan gebruik worden gemaakt van apparatuur voor gezichtsherkenning e.d. Het wetsvoorstel laat voor toekomstige ontwikkelingen dan ook alle ruimte. Voor zover door stelselmatige toepassing van deze middelen wordt opgenomen wat zich in een woning plaatsvindt, bijvoorbeeld door het plaatsen van een vaste camera die goed zicht heeft door de vooruit in een woning, dan is staande praktijk dat daarvoor – in de huidige wet op grond van artikel 20, derde lid, Wiv 2002 – ministeriële toestemming wordt gevraagd.[47] Echter ook anderszins kan sprake zijn van observatie. Zo is het regelmatig (dus met tussenpozen) of continu (zonder tussenpozen) raadplegen van hetgeen door een onderzoekssubject 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. In de PIA Wiv[48] wordt ter zake van deze vorm aangegeven dat *online* observatie niet alleen toekomstgericht is, maar ook tegelijk het verleden omvat (er kan immers ook worden gekeken wat in het verleden omtrent of door een persoon op internet is geplaatst); dit zou *online* observatie een principieel ander karakter geven dan observatie in de fysieke ruimte. Men pleit er dan ook voor dit afzonderlijk te regelen. We volgen de PIA Wiv op dit punt niet. Observeren is in onze ogen toch hoofdzakelijk een toekomstgerichte activiteit: het doel is toch primair om vast te stellen wat iemand gaat doen. Daarbij kan het gaan om zowel hetgeen in de fysieke ruimte afspeelt, maar ook in cyberspace. In het wetsvoorstel wordt voor onderzoek in cyberspace (in brede zin) overigens ook in andere bijzondere bevoegdheden voorzien, zoals het tappen van internetverkeer, het binnendringen in geautomatiseerde werken e.d., die met zware waarborgen zijn omgeven. Indien de uit te voeren activiteit het karakter heeft of krijgt van wat tot die bijzondere bevoegdheid wordt gerekend, zal die bijzondere bevoegdheid dienen te worden aangewend. Uiteraard zullen bij het observeren van wat een persoon op internet doet ook gegevens uit het verleden beschikbaar kunnen komen; dat is dan niet zozeer een vorm van observatie als hier bedoeld, maar valt naar ons oordeel onder de meer algemene bevoegdheid om uit

[47] Zie ook par. 7.1.6 PIA Wiv.
[48] Zie par. 7.1.5 PIA Wiv.

openbare bronnen (zoals het open deel van het internet) omtrent een persoon gegevens te verzamelen. Voor zover dit stelselmatig plaatsvindt is daaraan thans in artikel 38 een expliciete wettelijke grondslag gegeven. In die zin heeft deze vorm van observatie dan ook een gemengd karakter. Voor zover de uitoefening van deze bevoegdheid ook inhoudt dat men zich begeeft in de gesloten delen van sociale media en waarbij de daarmee belaste medewerker van de dienst zich bedient van een nepprofiel of een alias, dan is mede sprake van toepassing van artikel 41 en zal aan de aldaar gestelde eisen dienen te worden voldaan.

Ook bij het volgen van personen of zaken kunnen hulpmiddelen worden ingezet; het gaat dan om volgmiddelen, plaatsbepalingapparatuur en registratiemiddelen. Bij het volgen kan het gaan om het fysiek – bijvoorbeeld met een volgteam – volgen van een onderzoekssubject, het gebruik van bakens die GPS-coördinaten doorgeeft. Echter voor het volgen kan ook gebruik worden gemaakt van locatiegegevens die worden gegeneerd door het gebruik van mobiele communicatiemiddelen. In het laatste geval zal dan echter sprake zijn van een en–en situatie, te weten toepassing van de bijzondere bevoegdheid voor het volgen van een persoon (artikel 40) als het opvragen van toekomstige gegevens ex artikel 55 van het wetsvoorstel (verstrekking van *realtime* locatiegegevens).

Voor de uitoefening van de bevoegdheid ex artikel 40 is - buiten de in artikel 30, tweede en derde lid geregelde gevallen – de toestemming vereist van 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 (artikel 40, tweede lid).

Indien observatie- en registratiemiddelen als bedoeld in artikel 40, eerste lid, onder a, dienen te worden ingezet in woningen, kan daarvoor uitsluitend door de betrokken minister schriftelijk toestemming worden verleend aan het hoofd van de dienst (artikel 40, derde lid). Het verzoek daartoe dient ingevolge het derde lid, in aanvulling op het bepaalde in artikel 29, tweede 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 fysiek 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 58 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 58, derde 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 58 van het wetsvoorstel.

Van de toepassing van deze bevoegdheid dient ingevolge artikel 31 aantekening te worden gehouden. Ook de in artikel 59 geregelde notificatieplicht is, ingeval zonder toestemming van de bewoner een woning is betreden, van toepassing.

3.3.4.4.3 Agenten

Artikel 41 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 39 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 72 onderscheidenlijk artikel 73 van het wetsvoorstel geregeld.

In artikel 41, 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. Tevens is daarbij – vergelijkbaar met het bepaalde in artikel 39, vijfde lid, van het wetsvoorstel – bepaald, dat de bij of krachtens de wet geldende voorschriften betreffende de verstrekking van gegevens niet van toepassing zijn op de verstrekking van gegevens door een agent aan de dienst. Daarmee wordt duidelijk dat ook agenten gegevens aan de dienst kunnen verstrekken, indien de privacywetgeving dat hen normaal gesproken niet zou toestaan. Dit komt de rechtszekerheid ten goede.[49] Voor de inzet van een agent is toestemming vereist van de minister of namens deze het hoofd van de desbetreffende dienst; ook hier is ondermandaat mogelijk (artikel 41, tweede lid).Wel is in artikel 41, achtste 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 29, eerste 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 41, zevende 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.[50] 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

[49] Zie de reactie van de CTIVD op het concept-wetsvoorstel, pagina 56. Zie voorts CTIVD-rapport nr. 39, Onderzoek door de AIVD op sociale media, paragraaf 5.4.2.
[50] 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.

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 28, 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 30, eerste lid).

In artikel 41, vierde 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 41, vijfde lid; het zogeheten Tallon-criterium). In artikel 41, zesde lid, is bepaald wat in een instructie als bedoeld in het vierde lid dient te worden aangegeven. Zo zal duidelijk 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 (Kamerstukken II 2013/14, 33 820, nr. 2, pag. 7). Gelet hierop kan de delegatiegrondslag komen te vervallen.

Zoals in artikel 41, 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 41, derde 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 41, 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 41, negende 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 39, zesde 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.

3.3.4.4.4 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 een voorwerp gericht op de vaststelling van de identiteit van een persoon. Deze bevoegdheid wordt in vrijwel ongewijzigde vorm opnieuw geregeld in artikel 42 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 43 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 42, eerste lid, aanhef en onder c, de wettelijke grondslag.

Artikel 42

Artikel 42, 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 de uitoefening van de bevoegdheid is toestemming vereist van de minister of namens deze het hoofd van de desbetreffende dienst; ondermandaat is mogelijk (artikel 42, derde lid). Voor zover het een woning betreft[51], dient daarvoor door de voor de dienst verantwoordelijke minister schriftelijk toestemming te worden verleend aan het hoofd van de dienst. Het verzoek dient dan te worden gedaan door het hoofd van de dienst en dient in aanvulling op het bepaalde in artikel 29, tweede lid, het adres van de woning te bevatten die dient te worden doorzocht. De aldus verleende toestemming ziet

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

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 58, derde 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 45 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 42, 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. Het zomaar meenemen van voorwerpen is dan ook niet toegestaan. 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 bij betrokkene het vermoeden ontstaat 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 43

In artikel 43 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.[52] Uit de jurisprudentie van het EHRM[53] 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.[54] Met het voorgestelde artikel 43, 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.

[52] In de PIA Wiv (par. 6.2) wordt de interpretatie dat DNA-onderzoek reeds besloten zou zijn in artikel 22 Wiv 2002 twijfelachtig genoemd. In de memorie van toelichting op de huidige bepaling is daar immers – anders dan met betrekking tot vingerafdrukkenonderzoek – niets over gesteld, terwijl DNA-onderzoek indertijd volop in ontwikkeling was en ook in strafzaken reeds rond de eeuwwisseling uitvoerig is geregeld.
[53] EHRM 4 december 2008, *S. en Marper t. Verenigd Koninkrijk*.
[54] EHRM 4 december 2008, *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 43, eerste lid, van het wetsvoorstel zijn de diensten bevoegd tot het verrichten van DNA-onderzoek op basis van celmateriaal op voorwerpen ten behoeve van (a) het vaststellen alsmede (b) de verificatie van de identiteit van een persoon. Het doel is daarmee duidelijk afgebakend; DNA-onderzoek gericht op het afleiden van persoonskenmerken uit het genetisch materiaal is dan ook niet toegestaan.

Ten opzichte van het in consultatie gegeven wetsvoorstel is ervoor gekozen om deze twee doeleinden – identificatie en verificatie - van het door de diensten uit te (doen) voeren DNA-onderzoek afzonderlijk te benoemen; voorts wordt daarmee tegemoet gekomen aan hetgeen de CTIVD in haar toezichtsrapport (nr. 42) ter zake heeft gesteld. Daarbij wordt wel de kanttekening gemaakt dat – ondanks de aangebrachte scheiding – beide doeleinden in elkaars verlengde liggen en elkaar zelfs deels overlappen. In strafvordering wordt verificatie dan ook onder identificatie begrepen.

Bij *identificatie* gaat het primair om het vaststellen van de nog onbekende identiteit van een target (daaronder begrepen de situatie dat die identiteit nog onvoldoende vast is gesteld). Een door de diensten opgesteld DNA-profiel wordt daartoe vergeleken met DNA-profielen die de diensten in eigen huis hebben of met DNA-profielen die bij derden beschikbaar zijn (zoals bijvoorbeeld in de DNA-databank voor strafzaken of aan de hand van DNA-profielen verkregen van of in beheer bij collegadiensten). Dit kan onder meer voorkomen bij het vergelijken van DNA-profielen van terroristen die zich schuil hebben gehouden in *safe houses* in diverse landen. Bij de aanslagen in Parijs in november 2015 bleek dat diverse DNA-profielen een belangrijke rol speelden bij het identificeren van aanslagplegers en hun verblijfplaatsen.

Bij *verificatie (ook wel: toekomstige identificatie)* is bij de dienst bekend welke identiteit bij een door de dienst opgesteld en bewaard DNA-profiel behoort en wordt het DNA-profiel gebruikt om te verifiëren – aan de hand van een beschikbaar gesteld DNA-profiel of aan de hand van een opgesteld DNA-profiel met betrekking tot beschikbaar gekomen celmateriaal - of een bepaald target degene is van wie men vermoed wie het is, van wie door anderen wordt gesteld dat het een bepaalde persoon is of waarvan onbekend is wie het is, zoals bijvoorbeeld aan de hand van het afgenomen materiaal van een zelfmoordterrorist of het identificeren van een buitenlandse inlichtingenofficier hier ten lande.

Het DNA-onderzoek wordt verricht aan celmateriaal van een 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 42, 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 (waaronder begrepen het voorwerp met daarop mogelijk celmateriaal) te worden vermeld (artikel 43, derde lid onder b). Het celmateriaal wordt gebruikt voor het opstellen van de DNA-profiel.

In de PIA Wiv[55] wordt opgemerkt dat een voorwerp ook sporen van anderen kan bevatten. Los van de in de PIA gedane suggesties in de sfeer van organisatorische maatregelen, is het voorts van belang dat indien het voorwerp bij verwerving niet met zekerheid 1-op-1 te relateren is aan het target, daarvan aantekening te houden; dit raakt immers aan de betrouwbaarheid van het op basis daarvan vast te stellen DNA-profiel in relatie tot het target.

In artikel 43, vierde lid, wordt bepaald dat het DNA-onderzoek binnen drie maanden nadat het celmateriaal is vergaard, dient te worden uitgevoerd. Indien binnen deze termijn geen DNA-onderzoek kan plaatsvinden, dient het celmateriaal te worden vernietigd. Op verzoek van het hoofd van de dienst kan de termijn waarbinnen het DNA-onderzoek dient plaats te vinden eenmalig met een periode van ten hoogste drie maanden worden verlengd. In het verzoek dient de reden waarom het onderzoek niet binnen de reguliere termijn van drie maanden kan plaatsvinden te worden aangegeven.

Binnen drie maanden na het DNA-onderzoek dient vervolgens het celmateriaal, waaronder begrepen het voorwerp met daarop mogelijk celmateriaal, te worden vernietigd (artikel 43, vijfde lid). Van het vernietigen van het voorwerp dient te worden afgezien, indien dit overeenkomstig het bepaalde in artikel 42, tweede lid (overigens voor zover van toepassing), kan worden teruggeplaatst. 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.[56] 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.

[55] Par. 6.2 PIA Wiv.
[56] Zie ook EHRM 4 december 2008, *S. en Marper t. Verenigd Koninkrijk*, par. 120 en 121.

Het DNA-onderzoek vindt plaats met het oog op 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 de diensten zelf verwerken en voor (toekomstige) vergelijking opslaan.

De DNA-profielen die aldus beschikbaar komen, zijn voor een specifiek doel opgesteld (identificatie of verificatie) en mogen uitsluitend voor het onderzoek ten behoeve waarvan toestemming is verleend worden verwerkt. Verdere verwerking van DNA-profielen in het kader van andere onderzoeken van de dienst, 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 43, zesde lid). Verstrekking aan een buitenlandse collegadienst 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 jihadstrijders, de identiteit kan worden vastgesteld of geverifieerd. Voor zover een DNA-profiel aan een buitenlandse collegadienst wordt verstrekt, dient daarbij op grond van artikel 65, tweede lid, van het wetsvoorstel, altijd de zogeheten derde partij-regel te worden gesteld: te weten dat de gegevens die worden verstrekt aan die dienst, door die dienst niet aan derden mogen worden verstrekt. Ook overigens kunnen aan een verstrekking, indien daartoe aanleiding bestaat, voorwaarden worden gesteld omtrent bijvoorbeeld het gebruik dat ervan gemaakt wordt (zoals niet opnemen in een eigen databank of na een bepaalde periode vernietigen).

De voor een dienst opgestelde DNA-profielen mogen voor een periode van ten hoogste vijf jaren worden bewaard en dienen daarna te worden vernietigd. Het begrip DNA-databank voor de opgeslagen van de DNA-profielen bij de diensten dient te worden vermeden, aangezien dat slechts tot verwarring kan leiden; indien over de DNA-databank wordt gesproken bedoelt men immers regulier de DNA-databank voor strafzaken. De opslag van DNA-profielen bij de diensten staat daar geheel los van. De DNA-profielen worden overigens bij de diensten zelf bewaard en – voor zover het DNA-onderzoek bij het NFI is uitgevoerd - niet bij het NFI (waaronder begrepen de door het NFI beheerde DNA-databank voor strafzaken). Aan de opslag van de DNA-profielen zal in de in artikel 43, achtste lid, van het wetsvoorstel voorziene algemene maatregel van bestuur nadere eisen worden gesteld. Ook de toegang tot de DNA-profielen zal daarbij worden geregeld; die is overigens – ook zonder wettelijke voorziening ter zake – slechts voorbehouden aan (daartoe aangewezen medewerkers van) de diensten zelf. Derden hebben immers op geen enkele wijze toegang tot gegevens die door de diensten worden

verwerkt en die kan buiten de gevallen waarin de wet daar niet expliciet in voorziet (zoals aan de CTIVD in het kader van haar toezichthoudende taak) ook niet worden verleend.

De keuze voor een bewaartermijn van vijf jaren is ingegeven door een aantal factoren. Gelet op het met DNA-profielen voorgestane gebruik (waaronder verificatie) is het noodzakelijk deze voor een bepaalde termijn op te slaan. Een DNA-profiel wordt immers niet alleen gebruikt om de identiteit van een persoon te achterhalen, maar ook om deze te kunnen verifiëren als daarvoor reden is. Ter illustratie het volgende. Bij zogeheten uitreizigers (personen die op jihad gaan) is het zeer voorstelbaar dat zij voor langere tijd uit beeld verdwijnen, maar vervolgens alsnog, onder een alias (bijvoorbeeld nadat ze zich eerst dood hebben laten verklaren), naar Nederland terugkeren. Ook in het kader van het vaststellen van identiteit van (wellicht) uit Nederland afkomstige zelfmoordterroristen is het kunnen bewaren van het DNA-profiel voor een langer tijd van groot belang, nu hiervan ook na verloop van jaren sprake kan zijn. Bij de aanslagen in Parijs van november 2015 bleek dat het DNA-profiel een belangrijke rol speelde bij het identificeren van aanslagplegers en hun verblijfplaatsen. Dat is ook voorstelbaar in Nederland. Indien een DNA-spoor wordt gevonden op materiaal gerelateerd aan het conflict in Syrië, een beraming tot het plegen van terroristische misdrijven, etc. (wapens, springstoffen, restmateriaal van IED[57]s, basismateriaal voor het vervaardigen van ID's etc.) kan dit vergeleken worden met het DNA-profiel van bekende "terugkeerders" . Ook kan een vergelijking worden gemaakt met het belang van DNA-onderzoek in het kader van opsporing en vervolging van personen die zich schuldig hebben gemaakt aan strafbare feiten, omdat het kan wijzen op een verband tussen de aanwezigheid van de verdachte op een plaats delict. Ook voor de diensten is het niet zelden noodzakelijk verbanden te leggen tussen op locaties aangetroffen DNA-materiaal, aan de hand waarvan een DNA-profiel is opgesteld, met bij de diensten of derden beschikbare DNA-profielen. Voor een betere samenwerking in de bestrijding van terrorisme en bij de noodzakelijke ondersteuning van militaire missies is het voor de AIVD en MIVD noodzakelijk om met (beschikbare) DNA-profielen te kunnen werken. Op het gebied van contra-inlichtingenonderzoek is het voor de diensten eveneens noodzakelijk om met DNA-onderzoek en DNA-profielen te kunnen werken. Hierbij moet worden gedacht aan de situatie waarin inlichtingenofficieren van offensieve buitenlandse diensten met gebruikmaking van een pseudo-identiteit heimelijk activiteiten ontplooien in Nederland; ook hier kan het noodzakelijk zijn om met DNA-onderzoek en DNA-profielen te werken om de daadwerkelijke identiteit van betrokkene vast te stellen. Gelet op het voorgaande

[57] Improvised Explosive Devices.

is gekozen voor een bewaarperiode die aansluit bij de termijn die door de diensten wordt gehanteerd als de gemiddelde looptijd voor een onderzoek, te weten vijf jaar.

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 43, zevende lid). Hieraan is echter wel een maximum gesteld: de bewaartermijn mag in totaliteit niet meer dan dertig jaar bedragen.

Tot slot wordt opgemerkt dat een aantal aspecten verbonden aan het verrichten van DNA-onderzoek, de verwerking van DNA-profielen, waaronder begrepen de inrichting, het beheer en de toegang tot deze gegevens, en de omgang met celmateriaal, waaronder begrepen voorwerpen met daarop mogelijk celmateriaal, bij algemene maatregel van bestuur zullen worden geregeld. Artikel 43, achtste lid, biedt daarvoor de grondslag. De algemene maatregel van bestuur is onderworpen aan een zogeheten voorhangprocedure bij beide kamers der Staten-Generaal.

3.3.4.4.5 Openen van brieven en andere geadresseerde zendingen

In artikel 44 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 toestemming is vereist, in de regel van de voor de dienst verantwoordelijke minister of namens deze het hoofd van de desbetreffende dienst, is voor de uitoefening van deze bevoegdheid een last van de rechter vereist (artikel 44, 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 29, tweede 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 44, tweede 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 uitvoering van de aan de diensten opgedragen taak (artikel 44, derde 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 44, 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 42, eerste lid, van het wetsvoorstel, dan wel ingeval deze aan een instelling van post dan wel vervoer is toevertrouwd (artikel 44, vierde 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 44, vijfde 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 44, tweede 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.[58]

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 44, zesde lid). Met deze regeling wordt beoogd zeker te stellen, dat de uitlevering van de 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 44, zevende lid).

De uitoefening van de in artikel 44, eerste lid, geregelde bevoegdheid is in artikel 59 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 135 neergelegde geheimhoudingsplicht.

3.3.4.4.6 Verkennen van en binnendringen in geautomatiseerde werken

Algemeen

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 groot belang gebleken. Met het oog op het huidige dreigingsbeeld en het gegeven dat wij leven in een digitale wereld, is het voor diensten noodzakelijk om deze bijzondere bevoegdheid te kunnen uitoefenen. Het gebruik van digitale apparatuur zoals pc's, smartphones, laptops, tablets, maar ook de opslag in de cloud, is onmiskenbaar in alle facetten van het maatschappelijk leven (bij burgers, bedrijven en overheden) doorgedrongen en heeft daar een niet meer weg te denken positie verworven. Voeg daarbij de ontwikkeling van de Internet of Things

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

(waarbij apparaten, zoals koelkasten, auto's, horloges e.d. in toenemende mate worden gecomputeriseerd), waardoor onmiskenbaar blijkt hoe groot de impact van de digitalisering op de samenleving is. Bij targets van de diensten is toegang tot de smartphone of tablet tegenwoordig vaak relevanter dan bijvoorbeeld het binnentreden in een woning of het inzetten van een telefoontap. Bij onderzoek naar cyberaanvallen gericht op de Nederlandse infrastructuur of specifiek op de vitale sectoren is het belang om hetzelfde gereedschap te hebben als de digitale aanvaller. Zonder dit gereedschap, zijn de diensten niet staat om deze aanvallen (tijdig) te onderkennen.

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 de meeste 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 45 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.

Het begrip geautomatiseerde werk

Zowel bij de huidige als de voorgestelde bevoegdheden wordt met het begrip geautomatiseerd werk aangesloten bij hetgeen daaronder in artikel 80 sexies van het

Wetboek van Strafrecht (Sr) wordt verstaan.[59] Inmiddels is bij de Tweede Kamer der Staten-Generaal een voorstel van wet aanhangig tot wijziging van het Wetboek van Strafrecht en het Wetboek van Strafvordering in verband met de verbetering en versterking van de opsporing en vervolging van computercriminaliteit (computercriminaliteit III)[60], waarbij artikel 80sexies Sr opnieuw wordt gedefinieerd.[61] Indien dit wetsvoorstel (met inbegrip van het gewijzigde artikel 80sexies Sr) tot wet wordt verheven en werking treedt, zal de nieuwe begripsomschrijving ook bij de uitleg van het overeenkomstige begrip in onderhavig wetsvoorstel gelden.

Het is goed om op deze plek stil te staan bij de reikwijdte van het begrip geautomatiseerde werk, mede in het licht van de ontwikkelingen die sinds de inwerkingtreding van de huidige wet zich hebben voorgedaan en in de toekomst te verwachten zijn. Het gebruik van computers – in de verschillende verschijningsvormen (zoals pc-s, smartphones, laptops, tablets, maar ook de opslag in de cloud) - is onmiskenbaar in alle facetten van het maatschappelijk leven (bij burgers, bedrijven en overheden) doorgedrongen en heeft daar een niet meer weg te denken positie verworven. Voeg daarbij de ontwikkeling van de Internet of Things (waarbij apparaten, zoals koelkasten, auto's, horloges e.d. in toenemende mate worden gecomputeriseerd) aan toe, en het wordt duidelijk dat de reikwijdte van het begrip geautomatiseerd werk direct gevolgen heeft voor de reikwijdte van de bevoegdheid; dat is ook onder de huidige wet al zo. In de PIA Wiv (par. 7.2.3) wordt daar aandacht voor gevraagd. Het is echter inherent aan de gehanteerde definitie van geautomatiseerd werk (ook van de huidige definitie die door een uispraak van de Hoge Raad in 2013 al qua reikwijdte is verbreed) dat de ontwikkeling van apparatuur en systemen die aan die definitie voldoen daarmee ook onder de reikwijdte van de bevoegdheid komen te vallen. Dus dat kan betekenen dat de diensten ook slimme apparaten (zoals koelkasten, horloges, auto's e.d. die zijn uitgerust met computerfuncties) zouden kunnen *hacken*. Het is immers niet uitgesloten dat dergelijke slimme apparaten op enig moment gegevens verwerken die voor een goede taakuitvoering van de diensten noodzakelijk kunnen zijn. Vanuit het oogpunt van het totstandbrengen van een toekomstvaste regeling ligt het naar ons oordeel niet in de rede om hierop beperkingen te formuleren. De eisen die aan de uitoefening van de

[59] Op dit moment wordt daaronder verstaan: een inrichting die bestemd is om langs elektronische weg gegevens op te slaan, te verwerken en over te dragen. Volgens de wetsgeschiedenis zouden de functies van opslag, verwerking en overdracht dienen te worden beschouwd als cumulatieve voorwaarden; alleen apparaten die aan alle drie de voorwaarden zouden voldoen, zouden daar onder vallen (zoals stand alone computers). Inmiddels heeft de Hoge Raad in 2013 bepaald dat het begrip geautomatiseerd werk – met beroep op de wetsgeschiedenis – niet beperkt is tot apparaten die zelfstandig voldoen aan die functies, maar ook netwerken van computers en van geautomatiseerde inrichtingen voor telecommunicatie onder de reikwijdte van het begrip gebracht. HR 26 maart 2013, LJN BY 9718.
[60] Kamerstukken II 2015/16, 34 372.
[61] Voorstel voor een nieuw artikel 80sexies Sr: Onder geautomatiseerd werk wordt verstaan een apparaat of groep van onderling verbonden of samenhangende apparaten, waarvan er één of meer op basis van een programma automatisch computergegevens verwerken.

bevoegdheid tot het binnendringen in een geautomatiseerd werk worden gesteld, gecombineerd met ministeriële toestemming en een aan de uitvoering van de bevoegdheid voorafgaande bindende toets van de TIB, brengt naar ons mee dat er is voorzien in adequate waarborgen tegen oneigenlijk gebruik van deze bevoegdheid.

Het verkennen van technische kenmerken van geautomatiseerde werken die op een communicatienetwerk zijn aangesloten

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 45, eerste lid, onder a). Deze bijzondere bevoegdheid heeft ten opzichte van de bevoegdheid tot het binnendringen in een geautomatiseerd werk (artikel 45, 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 in het algemeen overwegend gebruikt door particuliere eindgebruikers voor verbindingen die een tijdelijk karakter hebben. 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 het onderzoek 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 het onderzoek gericht, efficiënt en zorgvuldig in relevante geautomatiseerde werken binnen te dringen. In de PIA Wiv (par. 7.2.6) wordt deze

bevoegdheid, met name door het feit dat deze semi continu wordt ingezet, aangemerkt als een vorm van observatie als bedoeld in artikel 40 van het wetsvoorstel. Naar ons oordeel gaat deze vergelijking niet op. Deze bevoegdheid wordt ingezet om de eigenschappen en karakteristieken van geautomatiseerde werken en de eventueel daaraan gekoppelde netwerken in kaart te brengen. Het is in zekere zin vergelijkbaar met een terreinstudie voorafgaand aan militaire inzet of een voorverkenning bij de mogelijke observatie van een object. Het betreft het in kaart brengen van de digitale infrastructuur. Het semi continu karakter komt bijvoorbeeld voort uit de noodzaak gedurende langere tijd in het kader van een militaire operatie de digitale *battlespace* in beeld te hebben. Wanneer verkenning er op gericht is te bezien of het haalbaar is om een geautomatiseerde werk binnen te dringen, heeft dit een kortstondig karakter.

Het binnendringen in het geautomatiseerde werk van een target en via een derde

In artikel 45, 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 *derden* binnen te dringen in geautomatiseerde werken die bij targets in gebruik zijn. Het geautomatiseerde werk is hier de corridor naar het geautomatiseerd werk van het target. Hiertoe wordt in artikel 45, 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.

Een ‘derde’ is in dit verband een technisch gerelateerde partij. Dat is dus een partij die technisch te relateren is aan het target. Daarbij moet onder andere gedacht worden aan een partij die een netwerk aansluit, een dienst levert, software levert of technische kennis levert. In de meeste gevallen zal die derde niet een individuele burger betreffen,

maar bijvoorbeeld een provider, tussenleverancier of dienstverlener. Dit betekent echter niet dat een individuele burger van dit begrip uitgesloten moet worden. In bijzondere gevallen moet het namelijk mogelijk zijn om het geautomatiseerde werk van een target binnen te dringen via een geautomatiseerd werk toebehorende aan een individuele burger. Hiervan kan alleen sprake zijn wanneer alternatieve, minder inbreukmakende manieren van binnendringen, niet succesvol zijn gebleken. Indien dergelijke gevallen zich in de praktijk voordoen zal in het verzoek om toestemming hieraan aandacht worden besteed.

Niet alleen in de PIA (par. 7.2.5) maar ook door diverse respondenten in de internetconsultatie zijn tegen de mogelijkheid van het binnendringen via het geautomatiseerde werk van een derde bezwaren aangevoerd; in hoofdstuk 12 van deze memorie van toelichting wordt daarop nader ingegaan. Desondanks zijn we van oordeel dat de mogelijkheid om via het geautomatiseerde werk van een derde toegang te krijgen tot het geautomatiseerde werk van het target gehandhaafd dient te blijven. In aanvulling op hetgeen hiervoor is gesteld, merken we ter zake nog het volgende op. De bevoegdheid tot het binnendringen in een geautomatiseerd werk van een target is niet of slechts zeer beperkt uitvoerbaar indien de mogelijkheid om via het geautomatiseerde werk van een derde toegang te verkrijgen niet toelaatbaar wordt geacht. In de praktijk verschaffen de diensten zich al in het overgrote deel van de gevallen toegang tot het geautomatiseerd werk van een target via het geautomatiseerd werk van een derde. Het internet is een ecosysteem van providers, tussenleveranciers en dienstverleners die ervoor zorgen dat informatie beschikbaar is via het internet. Een internetverbinding loopt via een ingewikkelde infrastructuur van routers, netwerkverbindingen, servers, e.d. Om toegang te krijgen tot het geautomatiseerd werk van het target moet gebruik kunnen worden gemaakt van die infrastructuur. De diensten zullen altijd eerst proberen rechtstreeks binnen te dringen in het geautomatiseerde werk van het target zelf. Indien dit niet mogelijk is kunnen alternatieven worden uitgewerkt, waaronder binnendringen via (een) geautomatiseerd werk van (een) derde(n).

Om eventuele twijfel over de toelaatbaarheid van het binnentreden via een geautomatiseerd werk van een derde weg te nemen, is besloten deze mogelijkheid expliciet in het wetsvoorstel op te nemen. Dit betekent niet dat deze mogelijkheid ongeclausuleerd kan worden toegepast. Het binnendringen van een geautomatiseerd werk van een derde zal te allen tijde moeten voldoen aan de vereisten van noodzakelijkheid, proportionaliteit en subsidiariteit. Dit betekent dat de inzet noodzakelijk moet zijn om bepaalde gegevens tijdig te verkrijgen. Als dezelfde gegevens op een andere manier ook zijn te verkrijgen, moet worden afgezien van het binnendringen van het geautomatiseerde werk via dat van een derde. Voorts moet het

doel dat wordt beoogd in verhouding staan tot de zwaarte van de bevoegdheid. De inzet van de bevoegdheid vindt dus enkel plaats indien zwaarwegende belangen van nationale veiligheid daartoe nopen. Er moet voorts – naast toestemming voor het binnendringen in het geautomatiseerde werk van het target – afzonderlijk toestemming worden gevraagd voor het binnendringen van het geautomatiseerde werk van de derde. Voor de derde moet de inzet van deze bevoegdheid voorts gepaard gaan met een zo klein mogelijke inbreuk op diens privacy. Zo mogen geen andere gegevens worden vergaard dan welke strikt noodzakelijk zijn voor het binnendringen van het geautomatiseerd werk van het target. De derde is immers niet meer dan een *stepping stone*. Tevens moet eventueel aangebrachte *malware* in het geautomatiseerd werk van de derde indien mogelijk worden verwijderd. Een daartoe strekkende inspanningsverplichting, die zich ook uitstrekt het geautomatiseerde werk van het target, is in artikel 45, zevende lid, van het wetsvoorstel vastgelegd. Er is gekozen voor een inspanningsverplichting, omdat in bepaalde gevallen het verwijderen van de *malware* disproportioneel nadeel zal opleveren voor de derde of voor zwaarwegende operationele belangen van de diensten. De CTIVD kan toezicht houden op de rechtmatige uitvoering van deze verplichting. Met de eerder genoemde introductie van een onafhankelijke toets vooraf door de TIB wordt bovendien gegarandeerd dat de (daadwerkelijke) uitoefening van deze zware bevoegdheid niet plaatsvindt zonder voorafgaande toestemming van een onafhankelijke instantie.

Inherente bevoegdheden

In artikel 45, 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 40, eerste lid en 47, 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 40, eerste lid) of het opnemen van de conversatie in een bepaalde

ruimte (artikel 47, 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 45, 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 40, eerste lid, en 47, eerste lid, kan de desbetreffende toestemming gelijktijdig worden aangevraagd.

Toestemming door de minister en aan de uitvoering voorafgaande bindende toets door de TIB

In artikel 45, 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 29, tweede lid. In aanvulling daarop dient ingevolge artikel 45, vierde lid, onder a, een omschrijving van de technische risico's verbonden aan de uitoefening van de desbetreffend bevoegdheid te worden gegeven. In de internetconsultatie hebben diverse respondenten erop gewezen dat het gebruiken van zwakheden in software of het zelf aanbrengen van technische hulpmiddelen (zoals *malware*) om toegang te verkrijgen tot een geautomatiseerd werk grote risico's kan opleveren voor de (andere) gebruikers van het geautomatiseerde werk maar ook voor gebruikers van dezelfde software waar een door de diensten onderkende zwakheid in zit. Indien de diensten dergelijke zwakheden onderkennen, kunnen anderen dat ook; ook kan door derden gebruik gemaakt worden gemaakt van door de diensten zelf aangebrachte *malware*. Het gebruik en misbruik van dergelijke kwetsbaarheden kan al naar gelang de systemen die het betreft grote maatschappelijke gevolgen hebben. Mede in het licht van het beleid van de overheid met betrekking tot cybersecurity (zie ook het recent ingediende voorstel van Wet gegevensverwerking en meldplicht cybersecurity[62]) kan dit vragen oproepen. Wij zijn ons van deze spanning bewust, maar

[62] Kamerstukken II 2015/16, 34 388.

het belang van de nationale veiligheid dient onder omstandigheden te prevaleren. Om echter bij de toestemmingverlening een gedegen afweging te kunnen maken wordt voorgeschreven dat de technische risico's verbonden aan het uitoefenen van de bevoegdheid (voor zover deze kunnen worden overzien) in beeld worden gebracht. Daarbij geldt tevens dat indien de diensten stuiten op significante kwetsbaarheden die de belangen van gebruikers op het internet kunnen schaden, het uitgangspunt is dat de diensten vervolgens de belangendragers, zoals het Nationaal Cyber Security Centrum, zullen informeren. Er kunnen echter wettelijke argumenten zijn (zoals bronbescherming of actueel kennisniveau) of operationele redenen zijn, die openbaarmaking van kwetsbaarheden (tijdelijk) in de weg staan. In artikel 45, vierde lid, aanhef en onder b, is voorts aangegeven dat (aanvullend) in een verzoek om toestemming tot uitoefening van de bevoegdheid, bedoeld in het eerste lid, aanhef en onder b, dient te worden aangegeven – voor zover van toepassing – welke van de onder het tweede lid genoemde bevoegdheden bij de uitoefening van eerstgenoemde bevoegdheid worden toegepast.

Een door de minister verleende toestemming dient ingevolge artikel 36, eerste lid, ter toetsing te worden voorgelegd aan de TIB. De uitoefening kan pas aanvangen nadat de TIB heeft geoordeeld dat de verleende toestemming rechtmatig is afgegeven.

Zoals eerder in de memorie van toelichting is aangegeven moet, indien het binnendringen in het geautomatiseerde werk van het target via een geautomatiseerd werk van een derde dient plaats te vinden, ook voor het binnendringen van het geautomatiseerde werk van een derde afzonderlijk toestemming dienen te worden verkregen (artikel 45, vijfde lid, verklaart hierop het derde en vierde lid van overeenkomstige toepassing). De reikwijdte van die bevoegdheid dient beperkt te blijven tot wat strikt daarvoor noodzakelijk is. De toepassing van de bevoegdheid als bedoeld in het tweede lid, aanhef en onder c (kort gezegd: aanzetten van camera of microfoon), zal daarbij niet noodzakelijk zijn en is dan ook expliciet uitgesloten.

Bijschrijfmogelijkheid

In artikel 45, achtste lid, wordt voorzien in de mogelijkheid dat in het geval dat toestemming is verleend tot het binnendringen in een geautomatiseerd werk van een target (persoon of organisatie) en het target op enig moment van een *ander* (aan hem toebehorend) geautomatiseerd werk gebruik gaat maken dat *in de plaats treedt* van dat andere geautomatiseerde werk, voor het binnendringen in dat (nieuwe) geautomatiseerde werk geen nieuwe toestemming is vereist. Ter illustratie: indien een target gebruik maakt van een smartphone en deze gedurende de periode waarvoor toestemming is verleend gebruik gaat maken van een andere smartphone , dan is het toegestaan ook in die nieuwe smartphone binnen te dringen. Een tweede situatie waar

deze mogelijkheid zich voor kan doen is als een target *naast* het in gebruik zijnde geautomatiseerde werk waarop de toestemming is verleend, *aanvullend* gebruik gaat maken of van een andere smartphone, tablet, laptop of digitale apparatuur. Het kan ook zijn dat het target al van een aanvullend digitaal apparaat gebruik maakt, maar dat het kenmerk pas wordt gevonden via het apparaat dat al onder de toestemming viel. Een target heeft niet alleen een smartphone, maar ook een tablet, laptop of andere digitale apparatuur. In de huidige digitale tijd wordt allerlei apparatuur door targets door elkaar heen gebruikt. In artikel 45, achtste lid, wordt tevens voorzien in de mogelijkheid dat in het geval dat de toestemming is verleend tot het binnendringen in een geautomatiseerd werk en het target op enig moment *naast* het geautomatiseerd werk waarvoor de toestemming is verleend, aanvullend gebruik gaat maken van een ander (aan hem toebehorend) geautomatiseerd werk, voor het binnendringen in dat (nieuwe) geautomatiseerde werk geen nieuwe toestemming is vereist.

De bijschrijfmogelijkheid ziet tevens op de bevoegdheid van binnendringen via het geautomatiseerde werk van een derde. Hierbij wordt benadrukt dat de toepassing van deze bevoegdheid aan dezelfde wettelijke beperkingen is gebonden als de bijschrijving van geautomatiseerde werken van targets. Zo kunnen enkel werken die in de plaats treden van, dan wel een aanvulling zijn op, het geautomatiseerde werk waar oorspronkelijk de toestemming voor is verleend, worden binnengedrongen. Zoals reeds toegelicht zal die derde in de meeste gevallen niet een individuele burger betreffen. Ter illustratie hiervan kan bijvoorbeeld gedacht worden aan een provider die vanwege een defect of uitbreiding een nieuw geautomatiseerd werk in gebruik neemt. In die bijzondere gevallen dat het binnendringen in een geautomatiseerd werk van een target plaatsheeft via het geautomatiseerde werk van een individuele burger kan aan eenzelfde situatie gedacht worden: een defect geautomatiseerd werk wordt vervangen.
In het verzoek tot toestemming tot het binnendringen in het geautomatiseerde werk van de derde wordt reeds een uitgebreide omschrijving van de technische risico's verbonden aan de uitoefening van de desbetreffende bevoegdheid gegeven. Indien deze risico's nopen tot het afzien van de inzet van de bevoegdheid ten aanzien van deze derde, zal geen toestemming worden verleend. Voor wat betreft het binnendringen van nieuwe onderkende geautomatiseerde werken van een derde zal, overeenkomstig het bepaalde in artikel 31 aantekening worden gehouden. Daarbij zal ook aantekening worden gehouden van de afweging van de technische risico's die in casu aan de uitoefening van die bevoegdheid verbonden zijn. De afweging van de technische risico's vindt niet alleen plaats ten behoeve van de bescherming van de belangen van de derde maar ook ten behoeve van de diensten zelf, die groot belang hebben bij het welslagen van ongezien binnendringen.

Medewerkingsplicht ontsleuteling

In artikel 45, negende tot en met twaalfde 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, elfde lid, van het Wetboek van Strafvordering. Op betrokkene rust ingevolge het elfde lid een medewerkingsplicht; het niet meewerken aan een verzoek is in artikel 141 van het wetsvoorstel strafbaar gesteld. Ten opzichte van de huidige medewerkingsplicht in artikel 24, derde lid, Wiv 2002 is het inroepen ervan procedureel verzwaard, doordat hiervoor thans ook afzonderlijk toestemming dient te worden verkregen van de betrokken minister (artikel 45, tiende lid). Voorts is deze toestemming onderworpen aan de rechtmatigheidstoets door de TIB. Aldus is de uitoefening van deze bevoegdheid aan een "dubbel slot" onderworpen.

Onderzoek op relevantie

Artikel 27 van het wetsvoorstel is onverkort van toepassing op de gegevens die door uitoefening van de bevoegdheid ex artikel 45, tweede lid, onder d jo. eerste lid, onder b, zijn verworven.

3.3.4.4.7 Onderzoek van communicatie

3.3.4.4.7.1 Algemeen

In paragraaf 3.2.5.6 van het wetsvoorstel (de artikelen 46 tot en met 57) 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. Dat betreft in de eerste plaats de uitbreiding van de reikwijdte van de bevoegdheden inzake telecommunicatie alsmede de daarmee corresponderende medewerkingsverplichtingen tot alle aanbieders van communicatiediensten. Daarnaast is voorzien in diverse wijzigingen die voortvloeien uit het kabinetsstandpunt met betrekking tot het onderdeel "Inzet bijzondere bevoegdheden in de digitale wereld"[63] uit het rapport van de Commissie Dessens, dat op 21 november 2014 aan de Tweede

[63] Hoofdstuk 5 van het rapport van de Commissie Dessens, *Evaluatie van de Wet op de inlichtingen- en veiligheidsdiensten 2002. Naar een nieuwe balans tussen bevoegdheden en waarborgen*.

Kamer is aangeboden. Dat betreft in het bijzonder de in de artikelen 48 tot en met 50 opgenomen regeling (onderzoeksopdrachtgerichte interceptie), 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 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. In de artikelen 51 tot en met 53 is een regeling getroffen inzake de informatie- en medewerkingsplicht voor aanbieders van communicatiediensten bij de verwerving van telecommunicatie op grond van de artikelen 47 en 48. Daarnaast is in aanvulling op de bestaande bevoegdheden 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 57 de medewerkingsverplichting tot ontsleuteling van communicatie opgenomen.

3.3.4.4.7.2 Aanbieders van communicatiediensten

Op dit moment wordt bij de uitoefening van de bijzondere bevoegdheden inzake onderzoek van communicatie, daaronder begrepen zowel de gerichte interceptie van telecommunicatie (artikel 25 Wiv 2002) als de verstrekking van telecommunicatiegegevens (artikel 28 en 29 Wiv 2002), de reikwijdte van de categorie instanties die kunnen worden verplicht om daaraan medewerking te verlenen beperkt tot de aanbieders van openbare telecommunicatienetwerken – en diensten. In artikel 1.1, onder ee en ff, van de Telecommunicatiewet (Tw) is gedefinieerd wat onder openbare telecommunicatienetwerken onderscheidenlijk openbare telecommunicatiediensten moet worden volstaan.[64] In de Tw is vervolgens geregeld dat deze aanbieders verplicht zijn om aan een dergelijk verzoek uitvoering te geven. Niet voldoen aan een dergelijk verzoek is als economisch delict strafbaar gesteld.

Sinds de inwerkingtreding van de Wiv 2002 heeft zich op het vlak van elektronische communicatie een enorme ontwikkeling voorgedaan waarvan het einde niet in zicht is.

[64] 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.

Niet alleen het gebruik van communicatiediensten als zodanig is spectaculair toegenomen, maar ook het aantal partijen dat deze en andersoortige communicatiediensten aanbiedt is enorm toegenomen. Niet alleen qua omvang (aantal dienstverleners) maar ook qua soort dienstverlening (vergelijk cloud-opslagdiensten, zogeheten OTT-diensten, Internet of Things, e.d.). Met betrekking tot deze nieuwe communicatiediensten is niet altijd duidelijk of die nu wel of niet onder het begrip openbare telecommunicatiediensten moet worden geschaard. Dat leidt enerzijds tot onzekerheid bij de diensten en de desbetreffende aanbieders waar het gaat om de vraag of ten aanzien van een verzoek om medewerking ook een plicht daartoe bestaat. Anderzijds moet worden geconstateerd dat het toenemende gebruik van nieuwe communicatiediensten ten koste van de "normale" communicatiediensten, denk daarbij met name aan OTT-diensten en het gebruik van bijvoorbeeld chatfuncties in games, de diensten voor steeds grotere problemen stelt om de voor een goede taakuitvoering noodzakelijke gegevens inzake de communicatie van targets te verkrijgen; temeer nu men – bij gebreke van een medewerkingsplicht die zich ook tot dergelijke diensten uitstrekt – is aangewezen op vrijwillige medewerking. Daarnaast vallen ook aanbieders van webhosts en besloten netwerken op dit moment niet onder de definitie van aanbieders van openbare telecommunicatienetwerken – of diensten als bedoeld in de Tw. 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 (opvragen verkeersgegevens en gebruikersgegevens), waarmee de hiervoor onderkende problematiek zou kunnen worden ondervangen, door introductie van het begrip "aanbieder van een communicatiedienst". Dit begrip is ontleend aan het Cybercrimeverdrag[65] en 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 biedt 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 onder meer die van besloten netwerken, webhostingsdiensten,

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

cloudopslagdiensten en de OTT-diensten. Ook het begrip "gebruiker van een dienst" is in dit kader nader gedefinieerd: de natuurlijke of rechtspersoon 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 46, aanhef en onder a onderscheidenlijk b, 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.

3.3.4.4.7.3 Onderzoek van communicatie met betrekking tot specifieke personen, organisaties, nummers dan wel technische kenmerken

Algemeen

Artikel 47 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 werk, ongeacht waar een en ander plaatsvindt. Het gaat daarbij om onderzoek van communicatie met betrekking tot specifieke personen, organisaties en nummers dan wel technische kenmerken ("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. Soms zal de uitoefening van deze bevoegdheid door de diensten zelfstandig kunnen plaatsvinden, bijvoorbeeld waar het gaat om de inzet van (richt)microfoons; in het merendeel van de gevallen, te weten bij de interceptie van telecommunicatie of gegevensoverdracht door middel van een geautomatiseerd werk, zal echter de medewerking van derden – in casu de aanbieders van communicatiediensten – vereist zijn.

Toestemmingverlening

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. In aanvulling daarop wordt in artikel 36 van het wetsvoorstel bepaald dat deze toestemming vervolgens dient te worden voorgelegd aan de TIB, die deze op

rechtmatigheid toetst (artikel 32, tweede lid); de uitoefening van de verleende toestemming kan pas aanvangen, indien de TIB van oordeel is dat de toestemming inderdaad rechtmatig is verleend. Zo niet, dan vervalt de toestemming van rechtswege. Hiermee is een extra waarborg ingebouwd voor de uitoefening van deze bevoegdheid. Indien de bevoegdheid dient te worden uitgeoefend jegens een journalist, waarbij de uitoefening kan leiden tot verwerving van gegevens inzake de bron van de journalist, dan wel jegens een advocaat, waarbij de uitoefening kan leiden tot verwerving van gegevens die betrekking hebben op de vertrouwelijke communicatie tussen een advocaat en diens cliënt, dan is ingevolge artikel 30, tweede, onderscheidenlijk derde lid, de toestemming van de rechtbank Den Haag vereist. Bovendien wordt de toestemming in laatstgenoemde gevallen verleend voor een periode van ten hoogste vier weken – met de mogelijkheid van verlenging voor telkens eenzelfde termijn - en niet voor de gebruikelijke termijn van ten hoogste drie maanden (met verlengingsmogelijkheid). De kortere toestemmingstermijn draagt niet alleen bij aan beperking van de inbreuk op het te beschermen rechtsgoed (bronbescherming journalist onderscheidenlijk de vertrouwelijke communicatie tussen een advocaat en cliënt), maar leidt er ook toe dat de noodzaak tot verdere inzet met kortere intervallen wordt geëvalueerd en de resultaten van de interceptie bij een verzoek om verlenging van de uitoefening van de desbetreffende bijzondere bevoegdheid, net als bij andere verlengingen van bijzondere bevoegdheden, nadrukkelijk wordt betrokken.

Het verzoek om toestemming dient te voldoen aan hetgeen in artikel 29, tweede lid, is bepaald en dient voorts in aanvulling daarop de in artikel 47, derde lid, bedoelde gegevens te bevatten. Dat betreft voor zover van toepassing, het nummer dan wel technisch kenmerk en 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 vereiste van het in het verzoek om toestemming vermelden van nummers en gegevens over de identiteit van de persoon of organisatie is ongewijzigd ten opzichte van het huidige artikel 25, vierde lid, Wiv 2002. Uit de wetsgeschiedenis blijkt dat ten tijde van het formuleren van de Wiv 2002 het begrip 'nummer' volstond voor de toenmalige vormen van gerichte interceptie. Onder nummer vielen conform de definitie in de Tw[66] immers voor de interceptie van vaste en mobiele telefonie (GSM) vereiste gegevens, zoals telefoonnummer, IMSI, IMEI en MSISDN, welke primair bedoeld waren voor toegang tot of identificatie van de gebruikers. Met de mogelijkheid tot het in het verzoek in plaats van een 'nummer' vermelden van een 'technisch kenmerk', wordt tegemoet gekomen aan de technologisch

[66] Artikel 1.1, onder bb, van de Telecommunicatiewet stelt dat onder een '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.

voortschrijdende praktijk, waarin communicatie niet langer enkel aan een nummer (bijvoorbeeld een telefoonnummer, IMSI, IMEI, MSISDN) gerelateerd wordt, maar dikwijls gekoppeld is aan een kenmerk dat niet valt onder de klassieke definitie van 'nummer' uit de Tw. Hierbij kan gedacht worden aan specifieke kenmerken die de diensten in staat stellen hun bevoegdheid tot interceptie gericht in te zetten, zoals credentials (user-ID's) van gebruikers van OTT-diensten en protocollen en parameters binnen bepaalde communicatiestromen. Deze gegevens kenmerken zich doordat zij vaak niet door de aanbieder aan de gebruiker zijn toegekend met als doel de gebruiker identificeerbaar te maken (zoals bijvoorbeeld wel het geval is bij een telefoonnummer), maar, al dan niet in samenhang met andere kenmerken - een uniek karakter hebben.

Het nummer 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 47, vierde lid, de bevoegdheid dan slechts mag worden uitgeoefend, indien het desbetreffende nummer of technisch kenmerk 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.[67] Waar het gaat om mobiele telefonie is dat niet altijd mogelijk, bijvoorbeeld in geval van prepaid 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 bijvoorbeeld door de inzet van een technisch hulpmiddel; een voorbeeld daarvan is – waar het gaat om mobiele telefonie – de inzet van zogeheten actieve scanapparatuur, zoals een IMSI-catcher[68]. 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 indien er sprake is van meerdere gebruikers binnen het bereik van de actieve scanapparatuur en andere, minder ingrijpende methoden, zoals scannen op verschillende locaties waar het target zich bevindt en aldus via vergelijking van de ontvangen nummers trachten het relevante nummer te onderkennen, niet mogelijk zijn vanwege bijvoorbeeld tijdgebrek (de urgentie van het onderzoek verzet zich ertegen) of

[67] Zie artikel 56 van het wetsvoorstel.
[68] 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.

bijvoorbeeld de wijze waarop en de soort communicatie die plaatsvindt. In verband hiermee wordt thans in artikel 47, 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.[69]

Voor wat betreft het achterhalen van het technisch kenmerk geldt eveneens dat hiervoor in voorkomende gevallen de medewerking van de aanbieder van de desbetreffende communicatiedienst kan worden ingeroepen. Daarenboven geldt dat de praktijk leert dat relevante technische kenmerken ook uit zelfstandig onderzoek van de diensten, dan wel uit de internationale samenwerking met buitenlandse collega-diensten, bekend kunnen worden. In die gevallen zal geen noodzaak bestaan de aanbieders op grond van artikel 52 of 56 dergelijke kenmerken te laten verstrekken, maar zullen de diensten zich op grond van artikel 53 wenden tot de aanbieders met de opdracht om medewerking te verlenen aan de uitvoering van de bevoegdheid tot gerichte interceptie op basis van het (reeds bekende) technische kenmerk.

Functiescheiding

In artikel 47, vijfde 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 het vierde lid – het gaat dan om

[69] 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.

het kennisnemen van de gegevens in het kader van de inzet van een technisch hulpmiddel als bedoeld in het vierde lid (zie hetgeen hiervoor is gesteld) - bij uitsluiting van anderen kennis mogen nemen van de inhoud van de ontvangen gegevens ter vaststelling van het juiste nummer.[70] Op deze wijze wordt bewerkstelligd dat van niet relevante communicatie slechts in beperkte kring kennis wordt genomen. In de praktijk is bovendien het gebruik van dergelijke apparatuur vanwege de technische kennis die het vereist, voorbehouden aan daarin gespecialiseerde medewerkers van de diensten.

NN-tap

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 47, zesde 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.

Bijschrijfmogelijkheid

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 slechts eenmalig van een bepaald nummer en toestel gebruik maakt. Om te voorkomen dat in dergelijke gevallen telkens opnieuw toestemming dient te worden gevraagd om 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 47, zevende 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

[70] Hiermee is ook uitvoering gegeven aan het advies van de CTIVD in haar reactie op het concept-wetsvoorstel (pag. 37).

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.[71] Het voorgaande is mutatis mutandis van toepassing ingeval de toestemming voor de uitoefening van de bevoegdheid als bedoeld in het tweede lid, plaatsvindt aan de hand van een technisch kenmerk.

Medewerkingsplicht

Bij de uitoefening van de bevoegdheid kan de medewerking worden ingeroepen van een aanbieder van een communicatiedienst. Daarbij dient onderscheid te worden gemaakt tussen de aanbieders van openbare telecommunicatienetwerken en –diensten en de andere aanbieders van communicatiediensten. Voor de eerstgenoemde groep geldt niet alleen dat de netwerken en diensten die zij aan het publiek aanbieden op grond van artikel 13.1 Tw op voorhand aftapbaar dienen te zijn, maar voorts dat zij op grond van artikel 13.2 Tw 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. Aangezien de Tw niet van toepassing is op de andere aanbieders van communicatiediensten is voor de andere aanbieders de medewerkingsplicht in het kader van onderhavig wetsvoorstel geregeld in artikel 51 e.v.. Daar komt bij dat deze categorie aanbieders geen met artikel 13.1 Tw vergelijkbare aftapbaarheidsplicht kennen en dus ook niet – zoals wel het geval is met betrekking tot de openbare netwerken en diensten[72] – op voorhand duidelijk is op welke wijze aan de plicht tot aftappen in technische zin invulling dient te worden gegeven. Ingeval dat aan een dergelijke aanbieder de opdracht wordt gegeven om aan een aan de dienst verleende toestemming tot interceptie medewerking te verlenen, dient ook duidelijk te zijn op welke wijze dat moet plaatsvinden; de opdracht aan de aanbieder zal ook daarover duidelijkheid geven. Hiertoe zullen de diensten in gezamenlijk overleg treden met de aanbieder.

In paragraaf 3.2.5.6.4 van het wetsvoorstel wordt voor deze categorie van aanbieders dan ook een samenhangende regeling getroffen, bestaande uit een informatie- en medewerkingsplicht bij de uitvoering van een verleende toestemming tot interceptie. Deze regeling is ook van toepassing bij de uitvoering van de hierna te bespreken bevoegdheid tot onderzoeksopdrachtgerichte interceptie. Ook wordt daar voorzien in een

[71] 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.
[72] Zie in dit verband het Besluit aftappen openbare telecommunicatienetwerken – en diensten en de regeling aftappen openbare telecommunicatienetwerken en –diensten.

regeling voor de kosten. In paragraaf 3.3.4.4.7.5 van deze memorie van toelichting wordt deze regeling nader toegelicht, zodat kortheidshalve daarnaar wordt verwezen.

Interceptie van militair verkeer met oorsprong of bestemming in het buitenland

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. Een met artikel 25, achtste lid, Wiv 2002 vergelijkbare maar in enkele opzichten gewijzigde regeling, is opgenomen in artikel 47, achtste lid, van het wetsvoorstel. Daarbij 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. In de PIA Wiv is uitvoerig stilgestaan bij de opmerking in de toelichting op het in internetconsulatie gegeven wetsvoorstel, dat van het stellen van het vereiste van toestemming was afgezien, omdat militair verkeer naar zijn aard niet vergelijkbaar is met het telecommunicatieverkeer tussen gewone burgers, omdat daarbij de persoonlijke levenssfeer van betrokkenen in het geding is. Uiteindelijk constateert men in de PIA Wiv dat er geen enorm grote maar wel enige privacyrisico's zijn gemoeid met gerichte interceptie van militair communicatieverkeer. In de PIA Wiv wordt derhalve voorgesteld om een toestemmingsvereiste op te nemen op ten minste het niveau diensthoofd. De interceptie van niet-kabelgebonden militaire communicatie, waarbij naar het oordeel van de PIA een lagere privacyverwachting bestaat of waar de interceptie beperkt is tot communicatiekanalen die alleen voor militaire doeleinden worden gebruikt, kan volgens de PIA toestemmingsvrij plaatsvinden. Mede naar aanleiding van deze aanbeveling is het oorspronkelijke voorstel heroverwogen, hetgeen ertoe heeft geleid dat thans alsnog voor de uitoefening van deze bevoegdheid een toestemmingsvereiste wordt gesteld ook voor dat deel van het militaire verkeer dat in de PIA is aangemerkt als toestemmingsvrij. De toestemming wordt verleend door het hoofd van de Militaire Inlichtingen- en Veiligheidsdienst voor zover bij de uitoefening daarvan geen medewerking van een aanbieder van een communicatiedienst is vereist; is dit laatste wel het geval, dan dient de minister toestemming te verlenen. Voorts wordt in de nieuwe regeling 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 20e 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 datastromen en communicatie van (wapensystemen van) strijdkrachten over door hen gebruikte verbindingsmiddelen 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-militair verkeer terstond dient te worden vernietigd.

Toets op relevantie

Op de gegevens die door toepassing van de bevoegdheid ex artikel 47 zijn verkregen is artikel 27 van het wetsvoorstel van toepassing.

3.3.4.4.7.4 Onderzoeksopdrachtgerichte interceptie van communicatie

Algemeen

In paragraaf 3.2.5.6.3 van het wetsvoorstel (de artikelen 48 tot en met 50) 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, te weten: onderzoeksopdrachtgericht onderzoek van communicatie. Hiermee wordt nadrukkelijk een koppeling gelegd met de Geïntegreerde Aanwijzing inlichtingen- en veiligheidsdiensten (GA) die op grond van artikel 6, eerste lid, van het wetsvoorstel door de Minister-president, Minister van Algemene Zaken, de Minister van BZK en de Minister van Defensie gezamenlijk wordt vastgesteld. In de GA zijn de concrete onderzoeksopdrachten voor de diensten opgenomen. Daarnaast kan er sprake zijn acute onderzoeksopdrachten, die eveneens op ministerieel niveau worden geaccordeerd. Onderzoeksopdrachtgerichte interceptie zal dus altijd in het kader van vooraf geformuleerde en geaccordeerde onderzoeksopdrachten plaatsvinden. 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). De voorgestelde regeling geeft uitwerking aan het kabinetstandpunt ter zake op het onderdeel "Inzet van bijzondere bevoegdheden in de digitale wereld" uit het rapport van de Commissie Dessens.[73] Bij de vormgeving van

[73] Kamerstukken II 2014/2015, 33 820, nr. 4.

de regeling is uitwerking gegeven aan het in het kabinetsstandpunt uiteengezette driefasenmodel. Daarnaast worden in paragraaf 3.2.5.6.4 van het wetsvoorstel een aantal met de uitoefening van deze bevoegdheid (en de bevoegdheid ex artikel 47; zie hiervoor) samenhangende bevoegdheden voor de diensten en daarmee corresponderende medewerkingsverplichtingen voor de aanbieders van communicatiediensten geregeld. Op hetgeen in laatstgenoemde paragraaf van het wetsvoorstel wordt geregeld, wordt in paragraaf 3.3.4.4.7.5 van deze memorie van toelichting ingegaan.

In de internetconsultatie is op de voorgestelde regeling door vrijwel alle respondenten forse kritiek geleverd. Dat betrof diverse aspecten van de voorgestelde bevoegdheid. In hoofdstuk 12 van deze memorie van toelichting wordt op die kritiek nader ingegaan. Een belangrijk kritiekpunt betrof echter de nut en noodzaak van de voorgestelde bevoegdheid: die zou niet dan wel onvoldoende zijn aangetoond. In het onderstaande zal eerst uitvoerig op deze kwestie worden ingegaan. Daarna zullen de verschillende onderdelen van de regeling worden toegelicht.

Nut en noodzaak van onderzoeksopdrachtgerichte interceptie

Algemeen

Nederland beschikt over inlichtingen- en veiligheidsdiensten (de AIVD en de MIVD) om dreigingen tegen onze samenleving tijdig te onderkennen, (inter)nationale belangen te verdedigen, de internationale rechtsorde te bevorderen en de krijgsmacht te ondersteunen. Ten behoeve van de uitvoering van hun taken zijn de diensten onder meer bevoegd kennis te nemen van telecommunicatie.

De Commissie Dessens heeft in het kader van de door haar uitgevoerde evaluatie geconstateerd dat de huidige wet aanpassing behoeft. Inlichtingen- en veiligheidsdiensten kunnen alleen dan hun rol in een democratische samenleving goed vervullen als ze over de juiste, noodzakelijke bevoegdheden beschikken. Zo heeft de commissie onder meer geconstateerd dat de bestaande interceptiebepalingen (artikel 26 en 27 Wiv 2002) te techniekafhankelijk zijn geformuleerd. Door de voortschrijdende technologie en nieuwe communicatiemogelijkheden zijn deze artikelen gedateerd[74]. Het huidige onderscheid tussen de ether en de kabel gaat niet samen met de snel voortschrijdende technologische ontwikkelingen op het gebied van dataverkeer en communicatie. Het huidige wettelijke systeem doet te weinig recht aan de noodzakelijke bevoegdheden in het kader van de nationale veiligheid. De potentiële gevolgen van

[74] Rapport van de Commissie Dessens, *Evaluatie Wet op de inlichtingen- en veiligheidsdiensten 2002. Naar een nieuwe balans tussen bevoegdheden en waarborgen*, p. 171.

medium- of techniekafhankelijke beperkingen zijn, aldus de commissie, te groot om te veronachtzamen[75].

Daarbij heeft de Commissie Dessens ook geconstateerd dat het toestaan van interceptie van kabelgebonden communicatie, evenals de interceptie van niet-kabelgebonden communicatie, een (potentiële) inbreuk maakt op de democratische vrijheden en grondrechten, zoals het recht op vrije communicatie en het recht op eerbiediging van de persoonlijke levenssfeer. Door de voortschrijdende technologie en de toegang tot een nieuw domein waarop de bevoegdheden worden toegepast, is het mogelijk om een groter bereik van data te ontsluiten en met meer geavanceerde methoden aan gegevensverwerving, - verwerking en dataopslag te doen. De Commissie Dessens heeft dan ook aangegeven dat de verruiming van bevoegdheden gepaard zal moeten gaan met een systeem van waarborgen om disproportionele aantasting van de democratische beginselen en grondrechten te voorkomen. De commissie merkt op dat inzet van bijzondere bevoegdheden ter bescherming van de nationale veiligheid niet altijd op gespannen voet hoeft te staan met het recht op vrije communicatie en de privacy van de burger. De inbreuk kan juist nodig zijn om de democratische beginselen en de grondrechten van burgers te beschermen tegen dreigingen die uitgaan van terroristische groeperingen, spionerende statelijke actoren en andere kwaadwillenden ten aanzien van de democratische beginselen en de grondrechten van diezelfde burgers.

De diensten moeten bij de inzet van deze bevoegdheid gebonden zijn aan een helder juridisch kader dat meer inzicht geeft in de voorwaarden waaronder en de manieren waarop de bevoegdheden ingezet mogen worden.

Het belang van onderzoeksopdrachtgerichte interceptie

In het huidige wettelijk kader bestaat er een onderscheid tussen gerichte interceptie (artikel 25: zowel kabelgebonden als niet-kabelgebonden telecommunicatie) en het intercepteren, verkennen en selecteren van niet-kabelgebonden telecommunicatie (artikelen 26 en 27: alleen niet-kabelgebonden telecommunicatie). Het verkennen, intercepteren en selecteren van kabelgebonden telecommunicatie is thans niet mogelijk. Het voorliggende wetsvoorstel breidt de bestaande bevoegdheid daartoe uit.

De AIVD en MIVD doen onderzoek naar een diversiteit aan thema's, zoals onder meer terrorisme, radicalisering, cyberdreigingen, bedreigingen voor de internationale rechtsorde alsmede in het kader van de ondersteuning van militaire missies en de politieke inlichtingen. Bij onderzoeksopdrachtgerichte interceptie zal de interceptie plaatsvinden ten behoeve van dergelijke onderzoeksgebieden waarbij de diensten zich

[75] Rapport van de Commissie Dessens, *Evaluatie Wet op de inlichtingen- en veiligheidsdiensten 2002. Naar een nieuwe balans tussen bevoegdheden en waarborgen*, p. 78.

richten op een geografisch gebied of op bepaalde datastromen. Om efficiënt en zorgvuldig onderzoek te kunnen doen binnen de diverse onderzoeksopdrachten hebben de diensten er baat bij om zoveel mogelijk zo gericht mogelijk data te verzamelen. Informatie die evident niet relevant is voor een onderzoek dan wel enig ander lopend onderzoek in het kader 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, zal zo spoedig mogelijk worden vernietigd; zie in dit verband artikel 48, vijfde lid, van het wetsvoorstel.

De ervaringen van buitenlandse inlichtingen- en veiligheidsdiensten waarmee de AIVD en MIVD in het kader van de nationale veiligheid samenwerken en die reeds beschikken over de mogelijkheid om kabelgebonden telecommunicatie te kunnen intercepteren, bevestigen de noodzaak om over deze bevoegdheid te beschikken teneinde een adequate informatiepositie op te bouwen en te behouden.

De eerste reden waarom deze toegang van belang is voor de informatiepositie van de diensten is dat door technologische ontwikkelingen de opbrengst van gerichte interceptie afneemt. Targets wijken uit naar open en anonieme opstijgpunten van het internet (zoals wifi-netwerken in hotels, restaurants en andere openbare ruimtes) waardoor een gerichte tap bij de traditionele aanbieders van telecommunicatiediensten in Nederland steeds minder effectief is. Targets passen bewust hun gedragingen aan om onder de radar te blijven, bijvoorbeeld door gebruik te maken van chatfuncties in games en van berichten- en videodiensten van social media. Het gaat hier onder meer om OTT-diensten. OTT-diensten verzorgen een dienst over het internet en ze hebben veelal communicatie- en (social) mediatoepassingen. Daarnaast zijn zij doorgaans goedkoper dan de traditionele methoden. Diverse OTT-diensten passeren de traditionele aanbieders van (mobiele) telefonie door bijvoorbeeld (video)bellen en chatten via het internet mogelijk te maken. Wereldwijd kunnen consumenten (en daarmee dus ook targets van de diensten) OTT-diensten benaderen door middel van alle denkbare digitale apparatuur zoals PC’s, laptops, spelcomputers, smartphones (Android, iOS en Windows Phone telefoons), muziekspelers, smart TV’s en tablets.

Satellietinterceptie is sinds decennia een belangrijke methode om buitenlandse telecommunicatie te verwerven die noodzakelijk is voor de goede taakuitvoering van de diensten. Daarbij gaat het om telecommunicatie waarmee inzicht wordt verkregen in geopolitieke ontwikkelingen en internationale crises, alsmede om telecommunicatie die noodzakelijk is voor de voorbereiding en uitvoering van militaire operaties en voor het contraterrorisme-onderzoek. Deze satellietinterceptie kan zich onder meer richten op telecommunicatie met betrekking tot het Midden-Oosten of Noord-Afrika. Dergelijke telecommunicatie is niet te verkrijgen via tussenkomst van aanbieders van

telecommunicatie in de landen van onderzoek, maar bovendien zal dergelijke (vrijwillige) medewerking veelal op operationele bezwaren van geheimhouding afketsen. Nu ook dergelijke communicatie in toenemende mate via de kabelgebonden infrastructuur gaat, is het noodzakelijk om de mogelijkheid tot onderzoeksopdrachtgerichte interceptie te verruimen tot kabelgebonden telecommunicatie.

In het voorgaande gaat het om tot op zekere hoogte *gekende* dreigingen, waarbij idealiter een aantal relevante actoren en nummers en/of technische kenmerken bekend zijn, op basis waarvan communicatie kan worden geselecteerd. Een doeltreffend inlichtingenproces vereist data om onderzoek te kunnen doen naar (aanvullende) relevante organisaties, personen, telefoontoestellen, computers etc. aan de hand waarvan communicatie kan worden geselecteerd. Historische gegevens zijn essentieel om met terugwerkende kracht verbanden te leggen en nieuwe kennis op te doen, maar ook om in het heden en naar de toekomst toe beter gegevens te kunnen duiden. Metadata-analyse en het verkennen zijn hierbij cruciale instrumenten. Daarmee kunnen nieuwe identiteiten worden ontdekt die van belang zijn in een onderzoek, evenals nieuwe telefoon-en IP-nummers ten behoeve van selectie. In vaktermen wordt dit het *target discovery and target development proces* genoemd. Het analyseren van de metadata is ook van belang om inbreuken op de persoonlijke levenssfeer, bestaande uit het kennisnemen van de inhoud van communicatie, zo min mogelijk te laten plaatsvinden.

De diensten hebben ook tot taak (nagenoeg) *ongekende* dreigingen op te sporen en handelend vermogen te creëren.

- Hierbij kan het onder meer gaan om nog niet onderkende terroristische cellen. Het is van belang om te weten of er vertakkingen zijn naar Nederland vanuit cellen in Frankrijk, België of Syrië/Irak.
- Het kan ook cyberdreigingen betreffen, zoals digitale spionage en de heimelijke beïnvloeding van ICT-systemen als onderdeel van hybride oorlogvoering (door bijvoorbeeld Rusland of Iran).
- Het kan gaan om de voorbereiding en ondersteuning van Nederlandse militaire operaties in een onbekende omgeving (zoals enige jaren geleden Uruzgan en thans Mali e.o., door IS ingenomen gebieden en in het kader van anti-piraterij).
- Ook wordt onderzoek gedaan naar de capaciteiten en intenties ten aanzien van specifieke landen en regio's op het gebied van massavernietigingswapens. Een dreiging kan bestaan uit de export van dual-use goederen naar een risicoland.

De beschikbaarheid van onderzoeksopdrachtgerichte interceptie, die gespecialiseerde onderzoekers van de diensten in staat stelt om op vooraf gesanctioneerde wijze analyses

te kunnen uitvoeren op deze onderzoeksterreinen, is voor de diensten een onmisbaar instrument om tijdig gekende en ongekende dreigingen bloot te kunnen leggen.

Daarnaast is nog het volgende van belang. De internationale samenwerking met buitenlandse collegadiensten komt onder druk te staan wanneer de Nederlandse inlichtingen- en veiligheidsdiensten niet een vergelijkbare informatiepositie hebben als andere diensten. Bij het teruglopen van de informatiepositie van de Nederlandse diensten, zal er minder worden samengewerkt. Andere Europese landen, zoals Frankrijk, Zweden en Duitsland, hebben de bevoegdheid tot kabelinterceptie voor hun inlichtingen- en veiligheidsdiensten. Indien de Nederlandse inlichtingen- en veiligheidsdiensten geen bevoegdheid krijgen voor onderzoeksopdrachtgerichte kabelinterceptie, heeft dit nadelige gevolgen voor de informatiepositie van de Nederlandse diensten en daarmee voor de veiligheid van Nederland.

In de huidige praktijk is een groot deel van de verwerving van communicatie in de ether gericht op volledig internationale telecommunicatie en op verkeer met oorsprong of bestemming in het buitenland. Dit zal bij onderzoeksopdrachtgerichte interceptie op de kabel ook het geval zijn**.** De onderzoeken naar de terreuraanslagen in Parijs van 7 januari 2015 (Charlie Hebdo) en 13 november 2015 (zestal aanslagen waaronder in de concertzaal Bataclan) en Brussel (24 mei 2014, Joods museum), maar ook de niet aflatende cyber(spionage)dreiging, laten zien dat ook situaties kunnen ontstaan die een toegang tot binnenlands verkeer noodzakelijk maken. Uit het onderzoek naar aanslagen zoals in Parijs van november 2015 is gebleken dat de plannen, de voorbereidingen en de uitvoering in verschillende landen werd gedaan. Aanslagen kunnen binnen de eigen landsgrenzen worden voorbereid om in het betreffende land toe te slaan, maar evenzeer om buurlanden te treffen. Onderzoek op binnenlands verkeer is derhalve noodzakelijk in het licht van zowel de interne dreiging als de dreiging richting buurlanden. Hieruit volgt dat onderzoeksopdrachtgerichte interceptie op binnenlands verkeer ook van groot belang kan zijn om de (ongekende) dreiging tijdig te kunnen onderkennen.

De noodzaak van onderzoeksopdrachtgerichte interceptie op het binnenlands verkeer blijkt zoals aangegeven ook uit de cyberdreigingen. De afgelopen jaren zijn meerdere bedrijven gehackt, waarbij kwetsbare of vertrouwelijke informatie (zoals intellectueel eigendom en persoonsgegevens) werd gestolen. Het cybersecurity-onderzoek van de diensten draagt bij aan het voorkomen dat de Nederlandse infrastructuur wordt misbruikt door diverse actoren voor digitale spionage, beïnvloeding, verstoring of andere ongeoorloofde activiteiten vanuit Nederland naar het buitenland, en verhoogt het weerstandsvermogen tegen dergelijke activiteiten gericht op de Nederlandse infrastructuur. Het kunnen verrichten van onderzoek aan data vergaard via

onderzoeksopdrachtgerichte interceptie is onmisbaar bij de attributie van digitale aanvallen (wie is de actor, op welke wijze geschiedt een aanval en met welke intentie?). Cybersecuritymaatregelen ondersteund door de toegang tot kabelgebonden infrastructuur draagt significant bij aan een veiligere digitale omgeving in Nederland.

De Wiv 2002 is tot stand gekomen in een periode waarin de huidige (digitale) ontwikkelingen nog niet bestonden of nog in de kinderschoenen stonden. Tegenwoordig verloopt 90% (of meer) van de telecommunicatie primair over kabelnetwerken. De huidige bevoegdheden, zoals neergelegd in de artikelen 26 en 27 Wiv 2002, hebben uitsluitend betrekking op niet-kabelgebonden telecommunicatie. Dat betekent dat de diensten van een zeer groot deel van de potentieel relevante telecommunicatie zijn uitgesloten. De diensten moeten over de capaciteiten beschikken om informatie op het juiste moment in het digitale domein te verwerven, te analyseren en daarover tijdig te rapporteren. De bijzondere bevoegdheid tot onderzoeksopdrachtgerichte interceptie in het kabelgebonden domein is daarbij onmisbaar. Alleen dan kunnen de diensten de (inter)nationale veiligheidsbelangen van Nederland en het optreden van de krijgsmacht adequaat ondersteunen. Het ontbreken van een goede eigenstandige inlichtingenpositie levert risico's op. Deze risico's kunnen onder meer bestaan uit een informatieachterstand op het terrein van het tijdig onderkennen van terroristische dreigingen. Voorts is het een risico om niet vroegtijdig digitale dreigingen te kunnen detecteren en afweren, zoals door technologische en/of economische spionage alsmede aanvallen op en het heimelijk beïnvloeden van Nederlandse informatiesystemen en infrastructuur. Dit leidt tot een gebrekkige uitvoering van digitale grensbewaking en landsverdediging. Een ander risico betreft de uitvoering van buitenlandse operaties van de Nederlandse krijgsmacht. Deze operaties worden onveiliger, minder goed voorbereid en minder effectief uitgevoerd dan mogelijk. Informatiegestuurd optreden blijft onderontwikkeld en de afhankelijkheid van coalitiepartners neemt enkel toe. Het niet (tijdig) onderkennen van de werkelijke intenties en capaciteiten van risicolanden, bijvoorbeeld op het gebied van massavernietigingswapens, territoriale expansie en militair vermogen, vormt een risico. Een volgend voorbeeld van de risico's wordt gevormd door het niet (tijdig) beschikken over een toereikende informatiepositie met betrekking tot internationale crises. Een laatste voorbeeld van de risico's van een informatieachterstand wordt zichtbaar doordat het digitale domein, of cyberspace, tegenwoordig ook een domein is voor militair optreden. De MIVD moet de veilige en effectieve inzet van de krijgsmacht ook in dit verband kunnen ondersteunen.

Het interceptieproces van onderzoeksopdrachtgerichte interceptie

Het uitgangspunt bij onderzoeksopdrachtgerichte interceptie is dat de diensten zo doelgericht en effectief als mogelijk te werk gaan, met zo min mogelijk inbreuken op de persoonlijke levenssfeer van burgers. Een dergelijke bijzondere bevoegdheid kan pas worden ingezet nadat een Geïntegreerde Aanwijzing inlichtingen- en veiligheidsdiensten (GA), op grond van artikel 6, eerste lid, van het wetsvoorstel door de Minister-president, Minister van Algemene Zaken, de Minister van BZK en de Minister van Defensie gezamenlijk is vastgesteld. De behoeftestelling voor de beide diensten wordt daarmee over de volle breedte van het takenpakket onderwerp van bespreking en weging in het CVIN en de RIV. De inhoud van de GA ziet 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.

Nadat de GA is vastgesteld worden door de diensten onderzoeksopdrachten opgesteld aan de hand van de toepasselijke wettelijke taak, waarin het doel en de noodzaak van het onderzoek is vastgelegd. Op grond van de onderzoeksopdracht wordt het onderzoek verricht. Indien het in het kader van het onderzoek nodig is om onderzoeksopdrachtgerichte interceptie in te zetten, geldt dat de interceptie alleen mag plaatsvinden met een vooromschreven doel en noodzakelijk moet zijn voor een goede uitvoering van deze wet (zie artikel 18, eerste lid, van het wetsvoorstel). Daarnaast moet de inzet proportioneel zijn en voldoen aan het vereiste van subsidiariteit (zie artikel 26 van het wetsvoorstel).

Doelgerichte verwerking van gegevens in relatie tot onderzoeksopdrachtgerichte interceptie

Met betrekking tot het interceptiestelsel geeft het begrip doelgerichte inzet in de eerste plaats een kader voor welke informatie wordt verworven. Het zal gaan om onderzoeksopdrachten zoals opgenomen in de Geïntegreerde Aanwijzing voor de beide diensten en om acute onderzoeksopdrachten die eveneens op ministerieel niveau zijn geaccordeerd. Onderdeel van onder meer deze 1e fase is het vernietigen van niet-relevante gegevens. Het doel zoals opgenomen in het verzoek om toestemming verschaft hiervoor de concrete handvaten. Dit is een belangrijke waarborg voor doelgericht optreden en het voorkomen dat de overheid meekijkt in willekeurige communicatie. Voorbeelden van mogelijke onderzoeksopdrachten zijn het verwerven van telecommunicatie inzake een concreet missiegebied en het verwerven van metadata tussen gebied in handen van terroristen en Nederland. Onderzoeksopdrachtgerichte interceptie vindt niet plaats om alle communicatie in de stad Den Haag een maand lang te verzamelen, om dan te bezien of voor de diensten relevante gegevens zijn binnengehaald.

De 2e fase van het interceptiestelsel heeft tot doel het optimaliseren van de opbrengst en het navolgende selectieproces (zie ook bijlage 4 bij het wetsvoorstel). De hypotheses op basis waarvan in deze fase wordt gewerkt, vormen een nadere invulling van het begrip doelgerichtheid. Een voorbeeld is het verwerken van gegevens om selectoren van *opposing forces* in het missiegebied te achterhalen of om nog ongekende contacten bloot te leggen tussen telefoontoestellen in een *failed state* en Nederland.

Ook in de 3e en laatste fase van het interceptiestelsel speelt doelgerichtheid een belangrijke rol. Om gegevens daadwerkelijk te kunnen selecteren en verwerken tot inlichtingenproducten zal wederom het doel gespecificeerd moeten worden in het verzoek om toestemming aan de minister. Dit kan bijvoorbeeld samenhangen met het verschaffen van handelingsperspectief aan politie en justitie, aan militaire commandanten, het NCSC of het bedrijfsleven alsmede het zelf kunnen treffen van maatregelen in het kader van contra-inlichtingenonderzoek.

Als de noodzaak, de doelmatigheid, de proportionaliteit en subsidiariteit is bepaald, zal toestemming worden gevraagd aan de desbetreffende minister(s) om de gevraagde vorm van onderzoeksopdrachtgerichte interceptie uit te mogen voeren voor een bepaalde periode. Na verkregen toestemming van de Minister van BZK dan wel van Defensie zal deze voor een rechtmatigheidstoets worden voorgelegd aan de TIB. Indien de TIB van oordeel is dat de toestemming rechtmatig is gegeven, kan met de onderzoeksopdrachtgerichte interceptie worden begonnen.

Het nieuwe normatieve kader voor onderzoeksopdrachtgericht onderzoek van communicatie

Het nieuwe normatieve kader voor interceptie en de daarbij op te nemen waarborgen kent de volgende elementen. Allereerst zal het technologieonafhankelijke stelsel voor de interceptie van telecommunicatie op hoofdlijnen uit een drietal fasen bestaan: (1) doelgerichte verwerving van telecommunicatie, (2) voorbewerking van de geïntercepteerde telecommunicatie en (3) (verdere) verwerking van de telecommunicatie. Deze drie te onderscheiden fasen komen grotendeels terug in onderscheidenlijk de artikelen 48 (verwerving), 49 (voorbewerking) en 50 (selectie en metadata-analyse) van het wetsvoorstel. Daarbij dient gerealiseerd te worden dat, zoals ook de CTIVD in haar reactie op het concept-wetsvoorstel in de consultatieronde heeft aangegeven, deze drie fasen nauw met elkaar zijn verweven. Ook de Afdeling advisering van de Raad van State verwijst daarnaar. Anders dan de CTIVD menen wij overigens dat de fasen op zich wel degelijk van elkaar zijn te onderscheiden, maar in de praktische uitvoering – onder meer vanwege het feit dat de resultaten van de ene fase betrokken zullen worden bij de wijze waarop de bevoegdheden in de andere fasen kunnen worden

uitgevoerd – zullen zij echter bij voortduring elkaar beïnvloeden. Zo zijn bijvoorbeeld de resultaten van de activiteiten in fase 2 (mede) van betekenis voor de toepassing van de bijzondere bevoegdheid tot verwerving als bedoeld in artikel 48 als de bijzondere bevoegdheid tot selectie als bedoeld in artikel 50. 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. Voorts is nog een extra waarborg toegevoegd, namelijk dat de ministeriële toestemming die in dit stelsel bij de uitoefening van de verschillende bevoegdheden is vereist, is onderworpen aan de rechtmatigheidstoets van de TIB (zie artikel 32, tweede lid, en 36, eerste lid, van het wetsvoorstel alsmede paragraaf 3.3.3 van deze memorie van toelichting). De CTIVD houdt achteraf toezicht op de rechtmatige uitvoering van deze bijzondere bevoegdheden. Bij de bespreking van de desbetreffende artikelen zal op de uitwerking van de hiervoor genoemde 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. 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 de opdracht tot medewerking; zie artikel 52 van het wetsvoorstel. Voorts is medewerking vereist bij de uitvoering van de opdracht, zij het dat daartoe niet eerder wordt overgegaan dan nadat ter zake met de desbetreffende aanbieder overleg is gevoerd; zie artikel 53 van het wetsvoorstel. In paragraaf 3.3.4.4.7.5 van deze memorie van toelichting wordt hier op ingegaan.

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. In dit verband is in artikel 60 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 48 is geïntercepteerd en het doel daarvan is het identificeren van personen of organisaties, dan is ook deze verwerking onderworpen aan ministeriële toestemming (artikel 50, vierde lid). Voor de volledigheid wordt opgemerkt dat ook ex artikel 49, met ministeriële toestemming, metadata-analyse kan plaatsvinden.

In het onderstaande zal thans op de verschillende fasen en de daarvoor relevante artikelen worden ingegaan. Voorts wordt verwezen naar bijlage 4 bij deze memorie van toelichting waarin de onderzoeksopdrachtgerichte interceptie (en de drie fasen) schematisch is weergegeven.

Fase 1: de doelgerichte verwerving van telecommunicatie (artikel 48)

In artikel 48, eerste lid, van het wetsvoorstel, is de bevoegdheid van de diensten neergelegd tot het met een technisch hulpmiddel onderzoeksopdrachtgericht aftappen, ontvangen, opnemen en afluisteren van elke vorm van telecommunicatie of gegevensoverdracht door middel van een geautomatiseerd werk ongeacht waar een en ander plaatsvindt, 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. Voorts mag ten behoeve van de technische analyse, voor zover noodzakelijk, de inhoud van de telecommunicatie of gegevensoverdracht uitsluitend worden gecontroleerd op de goede uitvoering van de ontvangst; bijvoorbeeld of hetgeen wordt geïntercepteerd niet bestaat uit ruis.

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.[76] 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[77]) 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, Wiv 2002). 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 57 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 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

[76] Zie Kamerstukken II 2004/05, 26 671, nr. 7, blz. 35.
[77] Zie ook hetgeen daaromtrent in paragraaf 3.3.4.4.6 van deze memorie van toelichting is gesteld.

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 onderzoeksopdrachtgerichte interceptie van etherverkeer 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 48, 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 29, tweede 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 mogelijk dienen te worden ingevuld. Op grond van artikel 48, derde lid, dient in het verzoek voor zover van toepassing de reden te worden gegeven waarom de uitoefening van de bevoegdheid ook betrekking dient te hebben op de inhoud van telecommunicatie of gegevensoverdracht door middel van een geautomatiseerd werk; dat betekent dus een extra motiveringseis ingeval niet met de interceptie van louter metadata kan worden volstaan. Voorts dient in het verzoek een typering te worden gegeven van de telecommunicatie of de gegevensoverdracht door middel van een geautomatiseerd werk ten aanzien waarvan de bevoegdheid dient te worden uitgeoefend. Uit het verzoek moet bijvoorbeeld blijken of het gaat om interceptie van etherverkeer dan wel kabelgebonden telecommunicatie. Voorts zal indien mogelijk, bijvoorbeeld wanneer targets van de diensten zich van specifieke middelen bedienen, 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 18 en 26 van het wetsvoorstel). De toestemming kan ingevolge artikel 48, tweede lid, worden verleend voor een periode van ten hoogste een jaar 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 aangewezen.

In artikel 48, 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 bij uitsluiting van anderen kennis mogen nemen van de ingevolge artikel 48, eerste lid, verworven gegevens. Het gaat daarbij om kennisneming in het kader van de in het eerste lid, tweede en derde volzin, geregelde bevoegdheid om de versleuteling ongedaan te maken alsmede het in het kader van de technische analyse controleren van de goede uitvoering van de ontvangst. 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 c.q. functiescheiding).

Tot slot is in artikel 48, vijfde lid, van het wetsvoorstel voorzien in een specifieke bewaartermijn van drie jaren ten aanzien van de ingevolge het eerste lid verworven gegevens en de gegevens waarvan de versleuteling ongedaan is gemaakt. 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 in relatie tot de huidige bevoegdheid ex artikel 27 Wiv 2002 (ongerichte interceptie van niet-kabelgebonden telecommunicatie) al jaren als een groot knelpunt ervaren. Teneinde deze problematiek te ondervangen wordt in het wetsvoorstel een maximale termijn van drie jaren voorgesteld.[78] Daarmee wordt afgeweken van de termijn van een jaar, zoals die is opgenomen in artikel 27, eerste lid, van het wetsvoorstel. De langere bewaartermijn van drie jaar hangt samen met de notie dat een integraal onderdeel van het inlichtingenproces wordt gevormd door analyse van historische data.

De diensten zijn zowel gericht op bekende als onbekende targets en worden daarbij tevens geconfronteerd met ongekende dreigingen die in kaart moeten worden gebracht. Hierbij kan gedacht worden aan het identificeren van een nieuw target, een niet nucleaire staat die nu de ontwikkeling van kernwapens nastreeft, een individu dat geïdentificeerd wordt als een (potentiële) terrorist of het ondersteunen van een nieuwe

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

militaire operatie. Vooral bij de onbekende targets en ongekende dreigingen is het essentieel om over een gedegen historisch archief te kunnen beschikken om tijdig dreigingen te kunnen onderkennen. Dit geldt voor alle onderzoeksopdrachten van de beide diensten en in het bijzonder voor de dossiers contra-terrorisme, de ondersteuning van militaire operaties, de proliferatie van (kennis van) NRBC[79] gerelateerde wapens en middelen en cyberdreigingen. Buiten het voorkomen van aanslagen en het (kunnen doen) mitigeren van bedreigingen, wordt van de diensten verwacht dat ook bij feitelijke aanslagen of cyberaanvallen, met terugwerkende kracht kan worden gereconstrueerd hoe een en ander feitelijk heeft kunnen gebeuren. Niet alleen om aan het licht te brengen wat er feitelijk gebeurd is en wie er voor verantwoordelijk zijn en wat de schade is (bijvoorbeeld bij cyberspionage), maar tevens om hiervan te leren en naar de toekomst toe beter in staat te zijn de veiligheid te waarborgen.

Ter illustratie volgt een aantal voorbeelden van de noodzaak van genoemde bewaartermijnen.

Op basis van een teruggekeerde Nederlandse jihadi, die voor meerdere jaren onzichtbaar is geweest voor de dienst als gevolg van zijn uitreis naar Syrië, kunnen bij terugkeer in Nederland door de dienst nieuwe inzichten worden verkregen. Als gevolg van deze nieuwe inzichten kan een onderzoek worden gestart met behulp van historische data, waardoor netwerken van ISIL kunnen worden gereconstrueerd die van groot belang zijn voor het vervolg van het contra-terrorisme onderzoek en het onderzoek naar in- en uitreizigers in het bijzonder.

Bij de terroristische aanslagen in Parijs in januari (Charlie Hebdo) en november (o.a. Bataclan, Stadion de France) 2015 heeft de AIVD in het kader van de eigen goede taakuitvoering en ter ondersteuning van de Franse collegadienst onderzoek gedaan. Onderzoek op basis van op dat moment beschikbaar gekomen informatie leidde tot unieke inzichten in een netwerk waarin zowel Nederlandse als Syrische kenmerken naar voren kwamen. Dit gebeurde aan de hand van historische data tot ruim twee jaar oud.

Landen van zorg proberen vaak via coverbedrijven proliferatiegevoelig materiaal te verwerven. Dergelijke bedrijven worden soms pas na enkele jaren onderkend door de westerse inlichtingengemeenschap. Wanneer de diensten in staat zijn om meerdere jaren terug te zoeken in vergaarde data, kan een beeld worden opgebouwd van wat deze bedrijven in de afgelopen jaren hebben getracht te verwerven en met wie ze in die periode contact hebben gehad. Hoe korter de periode is, hoe beperkter dit beeld zal zijn. Landen van zorg proberen daarnaast vanzelfsprekend de bouw van nucleaire installaties zo lang mogelijk geheim te houden. Zo is dit in een bepaald voorbeeld pas twee jaar na

[79] NRBC: Nucleair, Radiologisch, Biologisch en Chemisch.

feitelijke start van de activiteiten zichtbaar geworden en heeft het verder terug kunnen kijken de betrokkenheid van relevante actoren bloot kunnen leggen.

Besmettingen met *malware* worden veelal pas na geruime tijd opgemerkt. De snelheid waarmee deze *intrusions* worden gevonden is direct gerelateerd aan het vermogen van de diensten om breed te kunnen kijken naar mogelijke verdachte software. Voordat een bepaalde vorm van *malware* op een *high profile* target wordt ingezet, is het veelal al eerder getest geweest op "willekeurige" targets. Het detecteren van een dergelijke *intrusion* vindt dus al plaats op een moment dat de *malware* al geruime actief is en de voorbereidingen op de *intrusion* nog verder terug liggen in de tijd.

Schematisch komt dat op het volgende neer:

1. Op datum X wordt *malware/intrusion* op een overheidsnetwerk vastgesteld

2. Uit onderzoek blijkt de *malware* al 3 maanden (X-3) actief te zijn en gegevens te hebben gestolen,

3. Uit onderzoek blijkt verder dat de *malware* al drie maanden eerder op het netwerk van de overheidsinstantie gezet (X-6),

4. De aanval is uitgevoerd vanaf een server in Nederland waar de activiteiten tot anderhalf jaar terug X-18 zijn terug te voeren,

5. Onderzoek naar de modus operandi en de achterliggende actoren zal daarmee grotendeels gericht zijn op data die ouder is dan 18 maanden.

Historische data is dus ook voor *cyber defense* van belang. Daarnaast is deze data noodzakelijk om ook andere besmettingen van dezelfde *malware* en *intrusions* te onderkennen, die in het geheel nog niet onderkend zijn.

Een laatste voorbeeld is de inzet van de Nederlandse krijgsmacht in Uruzgan, waarbij de primaire focus lag op een beperkt deel van de provincie voor wat betreft de inzet van de eenheden, maar de Nederlandse commandant gebiedsverantwoordelijk was voor de gehele provincie. Voor bepaalde delen van de provincie werd minder intensief onderzoek verricht en bleef veel data onverwerkt omdat deze op dat moment minder relevant was. Als gevolg van de militaire planning en veranderde focus, moest de ondersteuning na verloop van tijd geïntensiveerd worden in deze eerder lager geprioriteerde gebieden. Om op een goede wijze invulling te kunnen geven aan de ondersteuning van deze militaire operaties is het van groot belang te kunnen beschikken over historische data om inzicht te krijgen in de bestaande netwerken en verhoudingen in deze "nieuwe" gebieden. De historische context draagt zorg voor een "warme start", waardoor de ondersteuning van

de militaire operaties het tempo van de militaire commandant kan volgen. Zonder deze historische context was dit in de praktijk onmogelijk gebleken.

Tijdens de ondersteuning van Taskforce Uruzgan is de MIVD regelmatig geconfronteerd met nieuwe Taliban commandanten, waar op dat moment nog geen kennis over aanwezig was. Onderzoek naar historische data toonde aan dat deze commandanten wel degelijk reeds jaren ervoor een rol speelden in de Taliban-netwerken. Doordat de dienst in staat was terug te kijken kon in korte tijd een beeld worden gevormd van de rol en positie van deze commandanten. Zonder deze historische context zou het maanden hebben geduurd alvorens een goed beeld van deze commandanten en andere relevante elementen kan worden opgebouwd, hetgeen in het operationele tempo van militaire missies niet verantwoord is.

Historische data is noodzakelijk om tijdig en gericht invulling te geven aan de inlichtingenbehoefte van de beide diensten. Het beperken van de mogelijkheden van de beide diensten om historische data te kunnen gebruiken zal de effectiviteit van het inlichtingenproces sterk degraderen. Een maximale bewaartermijn van drie jaar, zoals in het wetsvoorstel in artikel 48 is opgenomen, is gelet op de casuïstiek doeltreffend, met een acceptabel restrisico. De proportionaliteit is gewaarborgd door de doorlopende verplichting niet-relevant materiaal zo spoedig mogelijk te vernietigen en de additionele waarborgen in artikel 49 en 50.

De gegevens worden bewaard voor een gegevensverwerking als bedoeld in artikel 49 en 50.[80] Gegevens waarvan in dat kader is vastgesteld dat deze niet relevant zijn worden vernietigd. Gegevens die niet op hun relevantie zijn onderzocht, dienen uiterlijk na een termijn van drie jaren te worden vernietigd. Onder relevant voor het onderzoek wordt in lijn met het bepaalde in artikel 27, eerste lid, verstaan: relevant voor het onderzoek waarvoor de toestemming is verleend en in welk kader de gegevens aldus zijn verworven dan wel enig ander lopend onderzoek bedoeld in artikel 8, tweede lid, onder a en d, en de taken, bedoeld in artikel 10, tweede lid, onder a, c en e. Een bewaartermijn van drie jaar, zoals hier wordt voorgesteld, betekent overigens niet dat de vergaarde gegevens gedurende de gehele termijn van drie jaar worden bewaard en dan pas vernietigd. Hoewel hier, anders dan bij artikel 27, eerste lid, van het wetsvoorstel niet de plicht is opgenomen om de vergaarde gegevens zo spoedig mogelijk op hun relevantie te onderzoeken (hetgeen onder meer samenhangt met het feit dat de gegevens zowel voor een verwerking in het kader van artikel 49 als 50 relevant zijn en de (ir)relevantie in

[80] 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 aan buitenlandse collegadiensten – onder de daarvoor geldende voorwaarden en mits daarvoor toestemming van de voor de dienst verantwoordelijke minister is verkregen – kan plaatsvinden.

beide kaders dient te worden vastgesteld), vloeit uit de in artikel 18, eerste en tweede lid, van het wetsvoorstel neergelegde eisen voor gegevensverwerking (met name noodzakelijkheid, zorgvuldigheid en behoorlijkheid) reeds voort dat de diensten zo snel als mogelijk is tot datareductie komen teneinde de inbreuk die (mogelijk) gemaakt wordt op de persoonlijke levenssfeer van burgers zo beperkt mogelijk te houden. Daarnaast hebben de diensten vanuit het oogpunt van een werkbaar en efficiënt werkproces er geen belang bij om niet relevant materiaal voor langere tijd te bewaren.

Voor de gegevens waarvan de versleuteling nog niet ongedaan is gemaakt, wordt in artikel 48, zesde lid, voorzien in een bewaartermijn van eveneens drie jaren, zij het dat die termijn op een daartoe strekkend verzoek van het hoofd van de dienst aan de betrokken minister telkens met ten hoogste drie jaren kan worden verlengd. Daarmee is tegemoet gekomen aan hetgeen de Afdeling advisering van de Raad van State (onderdeel 4h van haar advies) opmerkt, namelijk dat het voorstel geen bepalingen bevat die zien op de termijn waarbinnen ontsleuteling moet plaatsvinden. De thans voorgestelde bewaartermijn van drie jaar is dan ook aan te merken als de termijn waarbinnen ontsleuteling plaats dient te vinden. Echter deze termijn kan worden verlengd, zij het dat daarvoor wel telkens toestemming van de voor de desbetreffende minister dient te worden verkregen. De mogelijkheid tot verlenging van de bewaartermijn wordt om de volgende redenen noodzakelijk geacht. Om vanuit een vercijferd bestand/bericht tot ontcijfering te komen kan een complex en daardoor langlopend proces zijn. De volgende stappen moeten daarbij doorlopen worden:

- er moet geanalyseerd worden welke product/applicatie gebruikt is;
- het gebruikte protocol en cryptografische algoritme(s) moeten achterhaald worden;
- voor de gebruikte algoritme(s) moeten cryptanalytische aanvallen worden ontwikkeld en geïmplementeerd;
- de cryptanalytische aanval(len) moeten worden uitgevoerd;
- de cryptanalytische aanvallen blijven achterwege als de informatie die leidt tot ontsleuteling op een andere wijze verkregen wordt.

Elk van deze stappen kan meerdere maanden of jaren in beslag nemen, afhankelijk van of al eerder naar de gebruikte apparatuur en/of cryptografische algoritme(s) onderzoek is gedaan. Om tot een succesvolle cryptanalytische aanval te komen is het van belang de vercijferde berichten lang genoeg te kunnen bewaren om alle stappen uit dit proces te kunnen doorlopen.

Voor sommige cryptosystemen kunnen berichten/bestanden pas gebroken worden als er voldoende materiaal beschikbaar is. Dan zijn er bijvoorbeeld duizenden vercijferde

berichten nodig, vercijferd onder dezelfde of gerelateerde sleutel om tot een succesvolle aanval op het gebruikte cryptografisch algoritme over te kunnen gaan. Het is hiervoor van belang de vercijferde berichten lang genoeg te kunnen bewaren tot er genoeg van zijn om de cryptanalytische aanval uit te kunnen voeren. Een bewaartermijn van drie jaar, met de mogelijkheid van verlenging, wordt hierbij dus ook bepaald door de frequentie van de (geïntercepteerde) gelijksoortig versleutelde berichten. Dat kan enkele weken zijn, maar ook enkele jaren.

Na afloop van de (eventueel verlengde) bewaartermijn worden de versleutelde gegevens vernietigd.

Fase 2: de voorbewerking van de geïntercepteerde communicatie (artikel 49)

De gegevens die op grond van artikel 48, eerste lid, zijn geïntercepteerd mogen verder worden verwerkt op de voet van het bepaalde in artikel 49 en/of 50. 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 49, 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.[81] Nu de interceptiebevoegdheid technologieonafhankelijk is geformuleerd en daarmee is uitgebreid tot het

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

kabelgebonden domein en waar het gaat om internetverkeer een dergelijke beperking geen betekenis heeft, is de beperking geschrapt.

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 identiteit van de persoon of organisatie behorende bij een telecommunicatie*. Deze vorm van search is primair gericht op de optimalisatie van de interceptie, waarbij vooral naar de aard van het verkeer wordt gekeken. Wordt datgene geïntercepteerd wat beoogd wordt? Hiertoe behoren ook processen zoals het onderkennen van bijvoorbeeld de taal van de communicatie(s). In veel gevallen kan dit worden uitgevoerd door geautomatiseerde processen, maar in sommige gevallen zal dit ook door menselijk handelen gebeuren. Search gericht op interceptie ziet dan ook vooral op de technische kenmerken en de aard van de communicatie, zoals protocollen, frequenties, taal maar ook de kwaliteit van de intercepties. In het kader van deze vorm van search 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 49, 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 48, 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. 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 is toestemming van de voor de desbetreffende dienst verantwoordelijke minister vereist (artikel 49, vierde lid). De toestemming voor de uitoefening van de bevoegdheid, bedoeld in het eerste lid kan

worden verleend op een daartoe strekkend verzoek van het hoofd van de dienst en wordt verleend voor een periode van ten hoogste een jaar en kan telkens op een daartoe strekkend verzoek worden verlengd. De inhoud van dit verzoek dient te voldoen aan de eisen van artikel 29, tweede 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 48 en een verzoek voor onderzoek als bedoeld in artikel 49, eerste lid, aanhef en onder a, in verband met het feit dat de ene bevoegdheid ondersteunend is aan de uitvoering van de ander; het betreft dan een zogenaamde combinatielast (of combi-last). De combinatielast is in de praktijk van de diensten geen onbekend verschijnsel. Toegespitst op de hier aan de orde zijnde bevoegdheden, wordt opgemerkt dat het ondenkbaar is dat uitsluitend een last voor interceptie (artikel 48) wordt gegeven en niet voor de uitoefening van de bevoegdheden in de andere fasen (artikelen 49 en 50). Intercepteren om te intercepteren is immers niet geoorloofd; interceptie vindt juist plaats met het oog op de uitoefening van de bevoegdheden tot search en selectie. Het ligt dan ook voor de hand (het verzoek om) toestemming voor combinaties van bevoegdheden te vatten in een gecombineerde last.

Dat laat onverlet dat de voor de uitoefening van deze bevoegdheden vereiste toestemming op de voorgeschreven wijze dient te worden verkregen; elk verzoek om toestemming dient aan de daaraan gestelde eisen te voldoen. Het is niet zo dat door de verzoeken om toestemming te combineren – dat uit praktische overwegingen aangewezen kan worden geacht, juist vanwege de verwevenheid van de diverse fasen – het met de in de wet gestelde eisen (zoals doelbinding, noodzakelijkheid, proportionaliteit en subsidiariteit) minder nauw genomen kan worden. Integendeel, die blijven voor elk verzoek om toestemming – ook gecombineerd - volledig van toepassing. Het verschijnsel combinatielast is niet meer net minder dan de combinatie van (de verzoeken om een) toestemming in één (verzoek om een) last in plaats van drie afzonderlijke (verzoeken om een) last(en).

Cybersecurity

De bevoegdheid van artikel 49, eerste lid, aanhef en onder a, is, in samenhang met de bevoegdheid van artikel 48, 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 48, eerste lid, geeft een regeling voor de daarvoor benodigde interceptie in het kabelgebonden domein en artikel 49, 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 (anomaliedetectie), 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 48, eerste lid, geïntercepteerde gegevens, gevormd, waarop vervolgens onderzoek plaatsvindt. In het tweede geval wordt bijvoorbeeld door de inzet van DPI-apparatuur[82], *real time* en online het dataverkeer geanalyseerd. De hier bedoelde netwerkmonitoring vindt door de diensten plaats ter uitvoering van, onder andere, 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 48 en 49 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 49, eerste lid) niet zonder de bevoegdheid tot kabelgebonden interceptie op grond van artikel 48, eerste lid, kan plaatsvinden, zal ook hier veelal sprake zijn van een combinatie-last.

Verkenning van telecommunicatie: search gericht op selectie

In artikel 49, 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 toestemming tot selectie ex artikel 50, tweede lid, de persoon of organisatie waarop de selectie kan worden toegepast reeds aangeduid. Op basis hiervan kan in de opbrengst van de geïntercepteerde telecommunicatie op zoek worden gegaan naar selectiecriteria die – mits navolgend op de voet van artikel 50, derde lid, vastgesteld – voor het onderzoek van de diensten naar die personen of organisatie relevante gegevens kunnen opleveren. Daarnaast kunnen potentiële selectiecriteria op hun bruikbaarheid worden geverifieerd door in de opbrengst van de geïntercepteerde telecommunicatie te bezien of deze relevante gegevens voor het onderzoek opleveren. Deze vorm van *search* gericht

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

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 opbrengst van de communicatie om te bepalen of met de selectiecriteria waarvoor toestemming is verkregen de gewenste informatie kan worden gegenereerd.[83] De tweede situatie die in artikel 49, 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 opbrengst van de communicatie om potentiële 'targets' te identificeren of te duiden.[84] 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 opbrengst van de 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 50, tweede lid, toestemming is gegeven.

Voor de uitoefening van de hiervoor geschetste bevoegdheden is op grond van artikel 49, 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 drie maanden. Deze termijn is – nu de hier bedoelde bevoegdheid ondersteunend is aan de bevoegdheid tot selectie - op de termijn die voor selectie geldt afgestemd. Dit verzoek dient te voldoen aan de eisen van artikel 29, tweede lid. De toestemming kan op een daartoe strekkend verzoek van het hoofd van de dienst worden verlengd.

Bij de uitoefening van de in artikel 49 geregelde bevoegdheden wordt kennis genomen van de inhoud van de ingevolge artikel 48 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 49, vijfde lid, is

[83] CTIVD rapport nr. 28, blz. 43.
[84] CTIVD rapport nr. 28, blz. 44.

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 48 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 49, 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 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 (*functiescheiding*).

Wordt bij het onderzoek als bedoeld in artikel 49, eerste of tweede lid, geconstateerd dat het gebruik 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 47, tweede lid, onderscheidenlijk artikel 50, 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 47, tweede lid, dienen te worden gedaan. De tweede situatie doet zich, zoals hiervoor al is geschetst voor, indien bij het *searchen* op de opbrengst van de telecommunicatie in verband met de toepassing van artikel 50 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 50, tweede lid, dienen te worden verkregen.

Fase 3: (verder) verwerken van de telecommunicatie (artikel 50)

Algemeen

In de derde fase vindt, zoals ook in de kabinetsreactie op het rapport van de Commissie Dessens ter zake is aangegeven[85], 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 en voor het onderzoek naar specifieke dreigingen. Tevens vindt in deze fase metadata-analyse plaats, welke gericht kan zijn op het identificeren van personen of organisaties. Artikel 50 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. Ingevolge artikel 48, vijfde lid, blijft de opbrengst van de 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 opbrengst aan gegevens kan worden geselecteerd. In aanvulling op hetgeen eerder over de bewaartermijn van drie jaar is gesteld, wordt nog het volgende opgemerkt. 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 waarvan de relevantie nog niet was vastgesteld, kunnen 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 tijdig afwijkingen van dat 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.

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

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 47 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 50, 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 48, 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 29, tweede lid, van het wetsvoorstel en dient - in aanvulling daarop – gegevens te bevatten betreffende de identiteit van de persoon of organisatie (dat vloeit overigens reeds voort uit artikel 29, tweede lid, maar is voor de volledigheid ook hier opgenomen) of een omschrijving van het onderwerp ten aanzien waarvan de bevoegdheid moet worden toegepast (artikel 50, tweede lid). 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 50, 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.[86] Het vaststellen van de selectiecriteria geschiedt door de voor de desbetreffende dienst verantwoordelijke minister of namens deze het hoofd. Het hoofd van de dienst kan aan hem ondergeschikte ambtenaren bij schriftelijk besluit 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.

Datareductie binnen het proces van onderzoeksopdrachtgerichte interceptie

In Nederland ligt bijna 100.000 km kabel in de grond. In elke kabel zitten tientallen fibers waarover de feitelijke datastromen lopen (zie bijlage 1). Zoals eerder in paragraaf 1.7 van deze memorie van toelichting is opgemerkt, wil de regering benadrukken dat er geen sprake van is dat een fors deel van de telecommunicatie van de Nederlanders zal worden opgeslagen. Onderzoeksopdrachtgerichte interceptie zal te allen tijde een zeer

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

klein percentage betreffen van het totaal aan nationaal en internationaal dataverkeer. De regering zal in 2017 één zogenaamde 'access-locatie' gereedmaken voor onderzoeksopdrachtgerichte interceptie. Het dreigingsbeeld is daarbij bepalend: bezien wordt op welk punt van de Nederlandse infrastructuur zal moeten worden aangehaakt om de noodzakelijke data te kunnen intercepteren. De diensten gaan niet over tot het opslaan of binnenhalen van alle datastromen. Op de access-locatie wordt alles in het werk gesteld om enkel data te verwerven die ten goede komt aan de onderzoeksopdrachten. Het verwerven geschiedt door de noodzakelijke datastromen te kopiëren en alleen met deze kopie vindt de verwerking door middel van onderstaand stappenplan plaats.

De datareductie binnen het proces van onderzoeksopdrachtgerichte interceptie is in de navolgende stappen te verdelen, waarbij gerealiseerd moet worden dat – zoals eerder opgemerkt – de drie hiervoor geschetste fasen op zich wel te onderscheiden zijn maar ook nauw met elkaar zijn verweven. Het proces wordt aan de hand van het voorbeeld van kabelgebonden interceptie uiteengezet. Het proces van satellietinterceptie is hieraan gelijk.

- *Het kiezen van de relevante fiber(s) (glasvezels) en kanalen*

De eerste reductieslag in het interceptieproces bestaat uit het identificeren van fibers die te relateren zijn aan één of meerdere onderzoeksopdrachten van de diensten. In de meeste fibers bevinden zich tientallen kanalen. Alleen die datastromen (en dus fibers) waarvan de gerede verwachting bestaat dat ze relevant zijn voor het beantwoorden van de onderzoeksopdrachten van de diensten worden gekozen. Deze beoordeling geschiedt aan de hand het zogenaamde 'snapshotten'. Hierbij wordt aan de hand van technische en inhoudelijke kenmerken onderzocht of de datastroom daadwerkelijk van belang is voor één of meerdere, concrete onderzoeksopdrachten. 'Snapshotten' kan vaker moeten plaatsvinden, omdat datastromen een dynamisch karakter hebben (vandaag relevant Syrisch verkeer over het ene kanaal, morgen over het andere) en de diensten alleen die kanalen willen/kunnen verwerken die van belang zijn voor het beantwoorden van de onderzoeksvragen (zie ook hetgeen eerder in deze memorie van toelichting is opgemerkt inzake de doelgerichte verwerking van gegevens in relatie tot onderzoekopdracht gerichte interceptie). Alle overige (en dus de overgrote meerderheid van alle) fibers en kabels in Nederland wordt niet geïntercepteerd. Binnen fibers worden bovendien enkel die datastromen verwerkt die daadwerkelijk te relateren zijn aan één of meerdere, concrete onderzoeksopdrachten.

- *Navolgende volumereductie*

De volgende stap in het verwerkingsproces bestaat uit het scheiden van metadata en inhoud in de datastroom van de gekozen kanalen. Aansluitend vindt een zo groot mogelijke volumereductie plaats. Dit is noodzakelijk omdat het ondanks bovengenoemde reductie nog steeds om heel veel data gaat. Om technische, operationele en privacyredenen is het van belang dit verder te reduceren, primair door de inhoud van communicatie binnen datastromen niet op te slaan. In de praktijk wordt alleen inhoud opgeslagen wanneer duidelijk is dat die in fase 2 en 3 van het interceptieproces noodzakelijk is en binnen concrete onderzoeksopdrachten valt. Ten eerste op grond van locatiegegevens, specifieke versleuteling, landcodes bij telefonie, cyberkenmerken of een specifieke communicatietoepassing (fase 2). Daarmee is niet gezegd dat de inhoud meteen zeer lang wordt bewaard. Afhankelijk van de omstandigheden kan het ook gaan om een week of enkele maanden. Daarnaast wordt inhoud opgeslagen op grond van het feit dat het aan selectiecriteria (fase 3) voldoet, zoals nummers. Metadata wordt in de regel bewaard, omdat het van groot belang is in tal van onderzoeken van de diensten, bijvoorbeeld om ongekende dreigingen te onderkennen. Wel wordt in deze fase nogmaals onderzocht of het binnen de kaders van een onderzoeksopdracht valt.

Ter illustratie van het vorenstaande kan het volgende voorbeeld dienen. Een kabel bevat 24 fibers met in totaal 480 kanalen. Van die 480 kanalen zijn er 3 kanalen relevant voor één of meerdere onderzoeksopdrachten en deze zijn verdeeld over 2 fibers. Enkel van deze 3 relevante kanalen (van de 480 op die specifieke kabel) wordt de data geïntercepteerd. Van de daadwerkelijk geïntercepteerde data wordt naar verwachting bij een eerste filtering 95% tot 98% direct weer verwijderd en vernietigd. Hierna volgt nog de hierboven genoemde volumereductie in fase 2 en 3.

- *Doorlopende vernietiging niet-relevant materiaal*

Bij het onderzoek van de diensten in fase 2 en 3 van het interceptiestelsel (artikel 49 en 50 van de wet) kan worden vastgesteld dat bepaalde geïntercepteerde gegevens op generlei wijze gerelateerd zijn aan onderzoeksopdrachten. Deze gegevens worden dan vernietigd. Dit is een voortdurend proces en vormt de laatste reductieslag in het interceptieproces. Uiteraard wordt alle data die niet geselecteerd is, vernietigd bij het verstrijken van de bewaartermijn.

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 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 55 van het wetsvoorstel. Dergelijke gegevens komen echter ook beschikbaar bij interceptie van telecommunicatie door de diensten, zoals bij de interceptie ex artikel 48, 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 deze onder omstandigheden veel aanwijzingen kunnen verschaffen over targets. Aan de hand van metadata kan in voorkomend geval worden vastgesteld of tussen telefoontoestellen contact is geweest, of e-mailadressen met elkaar verband houden, of IP-adressen met elkaar in contact staan en wanneer dat heeft plaatsgevonden, welke websites vanaf een PC zijn bezocht, waar een communicatiemiddel zich op een bepaald moment bevond e.d. Door analyse van deze gegevens, indien die kunnen worden gecombineerd met gegevens uit andere identificerende 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[87] 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 (daarbij kan het gaan om bijvoorbeeld een verkeerstechnische analyse die ziet op bijvoorbeeld transportaspecten zoals cell-id's, protocollen e.d.) 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 50, 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 60 ten aanzien van ingevolge artikel 48 verzamelde gegevens anders dan die welke de inhoud van de

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

desbetreffende telecommunicatie betreft. Artikel 60 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 worden toegepast (artikel 60, eerste en tweede lid). Zo kunnen ingevolge artikel 60, 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 50, 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 60, tweede lid, 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 29, tweede 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 60, 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 48, eerste lid, zijn verworven, kunnen op zich zelf staand worden geanalyseerd zonder dat daarbij andersoortige bestanden worden betrokken. Daarnaast is het mogelijk, en dat zal ook de praktijk zijn, dat metadata wordt gecorreleerd met andere gegevensbestanden die de diensten ter beschikking hebben. Voor zover dit gericht is op het identificeren van personen of organisaties, zullen voor zover van toepassing 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. Voor metadata-analyse in andere gevallen dan bedoeld in de eerste volzin van artikel 50, eerste lid, onder b, is geen toestemmingvereiste gesteld.

Waar het gaat om de bewaar- en vernietigingstermijn met betrekking tot de metadata, wordt verwezen naar het bepaalde in artikel 48, vijfde lid, en hetgeen daaromtrent eerder in deze memorie van toelichting ter zake is gesteld.

3.3.4.4.7.5 Informatie- en medewerkingsplicht aanbieders van communicatiediensten bij de verwerving van telecommunicatie op grond van artikel 47 en 48

Algemeen

Paragraaf 3.2.5.6.4 van het wetsvoorstel regelt een aantal bevoegdheden van de diensten en daarmee corresponderende plichten van aanbieders van communicatiediensten in verband met de uitoefening van de in artikel 47 en 48 van het wetsvoorstel geregelde bevoegdheden tot verwerving van telecommunicatie. Deze bevoegdheden zijn van essentieel belang om de in genoemde artikelen geregelde bevoegdheden tot verwerving van telecommunicatie op een goede wijze te effectueren. Het gaat daarbij om (1) de bevoegdheid van de diensten om aan een aanbieder van een communicatiedienst de opdracht te geven gegevens te verstrekken die noodzakelijk zijn om toepassing te kunnen geven aan de bevoegdheid tot gerichte interceptie en onderzoeksopdrachtgerichte interceptie, als bedoeld in artikel 47, eerste lid, onderscheidenlijk 48, eerste lid, en (2) de bevoegdheid van de diensten om aan een aanbieder van een communicatiedienst de opdracht te geven medewerking te verlenen aan de uitvoering van in genoemde artikelen geregelde bevoegdheden. De aanbieders zijn verplicht om aan deze opdrachten te voldoen. Voorts wordt in deze paragraaf voorzien in een regeling voor de vergoeding van de met de uitoefening van deze bevoegdheden verbonden kosten.

In artikel 51 van het wetsvoorstel is bepaald op welke aanbieders van communicatiediensten de in deze paragraaf opgenomen regeling van toepassing is. Daarbij dient onderscheid te worden gemaakt tussen de uitoefening van de bevoegdheid tot gerichte interceptie en de bevoegdheid tot onderzoeksopdrachtgerichte interceptie. Waar het gaat om de bevoegdheid tot gerichte interceptie is de regeling alleen van toepassing op die aanbieders van communicatiediensten op wie niet reeds op grond van artikel 13.2 van de Telecommunicatiewet een verplichting tot medewerking berust. Dat betekent dat in dit geval de regeling niet van toepassing is op aanbieders van openbare telecommunicatienetwerken en –diensten. Dat is niet nodig, omdat voor deze aanbieders geldt dat de door hen aangeboden telecommunicatienetwerken en –diensten op grond van artikel 13.1 Tw reeds aftapbaar dienen te zijn en dat een plicht tot medewerking aan een opdracht tot gerichte interceptie reeds in artikel 13.2 Tw is neergelegd. Waar het gaat om de uitvoering van de bevoegdheid tot onderzoeksopdrachtgerichte interceptie strekt de toepasselijkheid van de regeling zich uit tot alle aanbieders van

communicatiediensten. Hoewel men zou kunnen betogen dat artikel 13.2 Tw door zijn formulering ook in dit geval een medewerkingsplicht constitueert voor de aanbieders van openbare telecommunicatienetwerken en –diensten, ligt dat wetshistorisch niet voor de hand; de in hoofdstuk 13 Tw neergelegde regeling is immers opgezet met het oog op de uitoefening van (onder meer) de bevoegdheid tot gerichte interceptie.

Artikel 52: het verkrijgen van voor de uitoefening van de interceptiebevoegdheid benodigde gegevens en de plicht tot verstrekking

In artikel 52, 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 47, eerste lid, dan wel artikel 48, eerste lid, van het wetsvoorstel.

Het gaat dan allereerst om gegevens die nodig zijn om een verzoek tot toestemming tot interceptie als bedoeld in artikel 47, tweede lid, en artikel 48, tweede lid, adequaat te kunnen formuleren en – in het verlengde daarvan – een precieze omschrijving te kunnen geven van de medewerking die van de aanbieder wordt verlangd bij de uitvoering van de desbetreffende interceptiebevoegdheid. Immers, anders dan bij een opdracht tot medewerking bij gerichte interceptie aan een aanbieder van een openbare telecommunicatienetwerk – of dienst, is bij de aanbieders waarop onderhavige regeling van toepassing is, niet op voorhand duidelijk aan welke eisen zij dienen te voldoen bij het aftapbaar maken van hun communicatiedienst en op welke wijze de telecommunicatie bij de diensten dient te worden afgeleverd. Dit zal – mede afhankelijk van de aard van de communicatiedienst en de uit te oefenen bevoegdheid – telkens ad hoc dienen te worden bepaald. Het gaat dan om onder meer de technische gegevens van bijvoorbeeld het door de desbetreffende aanbieder geëxploiteerde telecommunicatienetwerk of dienst 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.

Daarnaast kan de bevoegdheid ex artikel 52, eerste lid, worden aangewend om gegevens te verkrijgen die bij kunnen dragen aan het in kaart brengen van het communicatielandschap[88], welke noodzakelijk is om op enig moment uitvoering te kunnen geven aan met name de interceptiebevoegdheid van artikel 48, eerste lid. Het in

[88] 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, karakteristieken van verkeersstromen en de belegging van communicatiekanalen.

kaart brengen van het communicatielandschap is noodzakelijk om de interceptiebevoegdheid ex artikel 48, eerste lid, 'doelgericht' in te kunnen zetten. Daartoe is het noodzakelijk om zo goed mogelijk inzichtelijk te krijgen welke aanbieder, waar in de infrastructuur, 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 gebruik van de door hen aangeboden netwerken en diensten.[89] Dit inzicht kan deels worden verkregen via uitoefening van de bevoegdheid ex artikel 49, 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 in artikel 52, eerste lid, neergelegde informatieplicht strekt zich uitsluitend uit tot de gegevens die de desbetreffende aanbieders 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 52, eerste lid, eerste volzin op te vragen beperkt tot die categorieën van gegevens die bij algemene maatregel van bestuur zijn aangewezen.

Voor het geven van de opdracht om gegevens te verstrekken is geen toestemming vereist. Er is daarvan afgezien, aangezien bij de gegevens waarop het verzoek betrekking heeft niet gaat om gegevens, waarbij de persoonlijke levenssfeer van concrete personen in het geding is. Het gaat hierbij voornamelijk om technische en bedrijfsmatige gegevens die zicht bieden in de door de aanbieder verzorgde communicatiediensten, hoe en waar communicatie verloopt e.d. Waar het gaat om de beoogde uitoefening van onderzoeksopdrachtgerichte interceptie kan het bijvoorbeeld betrekking hebben op de fysieke en logische inrichting van netwerken, routering en signaaleigenschappen.

De opdracht tot het verstrekken van gegevens wordt schriftelijk verleend door het hoofd van de dienst en dient ten minste de volgende gegevens te bevatten: (a) gegevens

[89] In zijn essentie vergelijkbaar met die welke in het kader van gerichte interceptie ex artikel 46 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.

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 de opdracht tot gegevensverstrekking is gericht, is ingevolge artikel 52, derde lid, verplicht aan het verzoek te voldoen. Het niet voldoen aan een dergelijk verzoek is in artikel 143 van het wetsvoorstel strafbaar gesteld. Op de verstrekking van de gegevens is artikel 39, vijfde 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 opdracht als bedoeld in artikel 52, eerste lid, worden gedaan. Voor een nadere toelichting op artikel 39, vijfde lid, wordt verwezen naar hetgeen daaromtrent is gesteld in paragraaf 3.3.4.3 van deze memorie van toelichting.

Tot slot is in artikel 52, vijfde lid, bepaald dat op het voldoen aan een opdracht 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.

Artikel 53: de plicht tot het verlenen van medewerking aan de uitoefening van de interceptiebevoegdheid

In artikel 53 wordt voorzien in de bevoegdheid van de diensten om de desbetreffende aanbieder van een communicatiedienst de opdracht te geven medewerking te verlenen bij (1) de uitvoering van de bevoegdheid tot gerichte interceptie ex artikel 47, eerste lid, waarvoor op grond van artikel 47, tweede lid, door de betrokken minister toestemming is verleend en (2) de uitvoering van de bevoegdheid tot onderzoeksopdrachtgerichte interceptie ex artikel 48, eerste lid, waarvoor door de betrokken minister ingevolge artikel 48, tweede lid, toestemming is verleend. De desbetreffende aanbieder is op grond van artikel 53, vijfde lid, verplicht om aan een opdracht te voldoen. Er is gekozen voor een medewerkingsplicht die zich tot alle aanbieders van communicatiediensten uitstrekt, aangezien in gevallen waarbij de nationale veiligheid in het geding is de diensten niet

afhankelijk dienen te zijn van vrijwillige medewerking. Het niet voldoen aan een opdracht is in artikel 143 strafbaar gesteld.

Overigens zal het niet in alle gevallen voor de diensten noodzakelijk zijn om de medewerking van een aanbieder van een communicatiedienst in te roepen bij de uitoefening van de bevoegdheid tot onderzoeksopdrachtgerichte interceptie van telecommunicatie. Zoals bekend beschikken de diensten thans over een eigen satellietgrondstation in Burum, waar men zelfstandig niet-kabelgebonden telecommunicatie intercepteert. Indien deze capaciteit beschikbaar is en ingezet kan worden bij de uitoefening van een verleende toestemming tot uitoefening van de bevoegdheid ex artikel 48, eerste lid, van het wetsvoorstel, ligt het voor de hand om daarvan gebruik te maken. 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 uitoefening van de in artikel 53, 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. Het verzoek om toestemming dient in aanvulling op het bepaalde in artikel 29, tweede 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.

De toestemmingstermijn voor het inroepen van de medewerking van de aanbieder is afgestemd op de duur van de toestemmingstermijn die wordt gehanteerd bij de uitoefening van de desbetreffende interceptiebevoegdheid. Dit betekent dat de toestemming wordt verleend voor een periode van ten hoogste drie maanden, indien de medewerking is vereist met betrekking tot de uitoefening van de bevoegdheid tot gerichte interceptie (artikel 47, eerste lid). Indien de medewerking betrekking heeft op de uitoefening van de onderzoeksopdrachtgerichte interceptie (artikel 48, eerste lid) kan de toestemming worden verleend voor een periode van ten hoogste een jaar. Het ligt voor de hand dat de termijn voor toestemming voor de uitoefening van de interceptiebevoegdheid en de toestemming tot het verlenen van een opdracht om daaraan medewerking te verlenen op elkaar worden afgestemd. In beide gevallen kan telkens op een daartoe strekkend verzoek voor eenzelfde periode de toestemming worden verlengd (artikel 53, derde lid). De toestemming voor het kunnen geven van een opdracht tot medewerking is dus vereist naast de toestemming die ingevolge artikel 47,

tweede lid, en 48, tweede lid, voor de interceptie als zodanig is vereist. Een afzonderlijke toestemming om de medewerking van een aanbieder bij de uitoefening van de hier bedoelde bevoegdheden in te roepen, is vereist, omdat daarbij tevens dient te worden vastgesteld welke soort medewerking van de aanbieder wordt verlangd (maatwerk).

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.[90] 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 53, 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 en ter zake van hem de medewerking als bedoeld in artikel 53, eerste lid, in te roepen, is het in het algemeen wenselijk dat voor een beperkte periode, te weten tot een jaar na afloop van de periode waarvoor de opdracht als bedoeld in artikel 53, eerste lid, is verleend, 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

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

desinvestering aan de kant van de aanbieder voorkomen. In artikel 53, zesde lid, is overigens wel voorzien in de mogelijkheid tot het verlenen van ontheffing aan een aanbieder van de verplichting, bedoeld in de eerste volzin. Indien instandhouding van de technische voorzieningen geen enkel redelijk doel meer dient, bijvoorbeeld in het geval dat de dienst te kennen heeft gegeven geen gebruik meer van de technische voorzieningen te zullen maken, moet een dergelijke ontheffing mogelijk zijn.

In artikel 53, zevende lid, is een regeling opgenomen voor de vergoeding van de door de aanbieder te maken kosten. De aanbieder die ingevolge artikel 53 verplicht is medewerking te verlenen aan de uitvoering van een opdracht als bedoeld in het eerste lid, heeft naar redelijkheid aanspraak op vergoeding van uit 's-Rijks kas van de investerings-, exploitatie- en onderhoudskosten voor de technische voorzieningen die zijn of worden gemaakt teneinde te kunnen voldoen aan de opdracht, alsmede van de door de aanbieder gemaakte administratie- en personeelskosten rechtstreeks voortvloeiend uit het voldoen van de opdracht. In de internetconsultatie, maar ook in de PIA Wiv (zij het vanuit een andere invalshoek, te weten het daaraan verbonden privacyrisico), was ernstige kritiek geuit op de in het concept-wetsvoorstel opgenomen regeling inzake de kostenverdeling. Daarbij was aansluiting gezocht bij artikel 13.6 Tw; de kosten voor de treffen technische voorzieningen zouden in dat geval geheel bij de desbetreffende aanbieder worden gelegd. Naar aanleiding van de diverse kritiek is de eerder voorgestelde regeling heroverwogen en is besloten om ook deze kosten naar redelijkheid te vergoeden. Zie ook hetgeen daaromtrent is gesteld in hoofdstuk 11 van deze memorie van toelichting. Tot slot is in artikel 53, achtste lid, bepaald dat bij ministeriële regeling regels worden gesteld met betrekking tot de vaststelling en de vergoeding van de kosten, bedoeld in het zevende lid. Bij de uitwerking van deze regeling zal grotendeels aansluiting worden gezocht bij de inhoud van de Regeling kosten aftappen en gegevensverstrekking die op grond van artikel 13.6, derde lid, Tw is vastgesteld.

3.3.4.4.7.6 Informatieverzoeken en medewerkingsplicht met betrekking tot telecommunicatiegegevens

Algemeen

In paragraaf 3.2.5.6.5 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 55 en 56, 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). De bevoegdheid in artikel 54 van het wetsvoorstel is nieuw en ziet onder meer op het opvragen van de telecommunicatie van een gebruiker die door de aanbieder als onderdeel van de door hem verleende communicatiedienst is opgeslagen.

Het opvragen van bij een aanbieder van een communicatiedienst opgeslagen telecommunicatie van een gebruiker alsmede het opvragen van gegevens bij een persoon of instantie die in het kader van de uitoefening van een beroep of bedrijf de opslag verzorgt van door derden via geautomatiseerde werken verwerkte gegevens (artikel 54)

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 wordt in toenemende mate gebruik gemaakt van zogenaamde webbased-toepassingen zoals de cloud.[91] 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 gegevens van gebruikers van die clouddiensten op te vragen. Het kan daarbij gaan om de situatie dat de aanbieder van een communicatiedienst *als onderdeel van de door hem verleende communicatiedienst* aan de gebruiker de telecommunicatie van die gebruiker opslaat (bijvoorbeeld webmail[92] of voicemail[93]); daarnaast is er de situatie mogelijk dat sprake is van opslag van door derden via geautomatiseerde werken verwerkte gegevens, *welke geen onderdeel is van een verleende communicatiedienst*, en waartoe voor die derde rechtstreeks geautomatiseerde toegang bestaat (het gaat dan om een vorm van externe opslag van bestanden). Aldus blijkt dat er diverse manieren

[91] 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.

[92] Onder webmail wordt een webapplicatie verstaan die het mogelijk maakt e-mail te gebruiken via een webgebaseerde gebruikersinterface. Het is te gebruiken als een gewone website, waardoor het mogelijk is om het overal ter wereld te gebruiken zonder een apart e-mailprogramma te installeren.[92] Ook wordt deze dienst aangeboden door aanbieders van internettoegang, waarbij men naast de internettoegangsdienst regulier ook een e-maildienst (waarvoor een e-mailprogramma dient te worden geïnstalleerd) aanbiedt met inbegrip van de mogelijkheid van webmail. Bij webmail wordt de mail van een gebruiker van een gebruiker (ontvangen e-mail, verzonden e-mail, concepten e.d.) bij de desbetreffende aanbieder opgeslagen.

[93] Voicemail is een vorm van dienstverlening ter vervanging van een eigen antwoordapparaat. De desbetreffende voorziening bevindt zich op een platform in een vast of mobiel telefoonnetwerk. Oproepen die door de opgeroepen persoon niet worden aangenomen, worden doorgeschakeld naar het voicemailplatform, waarna er door de beller een bericht achtergelaten kan worden. Op een later momnet kan de opgeroepen persoon het achtergelaten bericht alsnog beluisteren.

van opslag van gegevens in de cloud mogelijk zijn. [94] Sommige diensten van de verschillende aanbieders lopen in elkaar over. Zo zijn er aanbieders van internetdiensten die opslagdiensten in de cloud aanbieden. Webmaildienstenworden niet alleen gebruikt om berichten te versturen naar andere e-mailadressen maar worden ook voor interne communicatie binnen bijvoorbeeld terroristische groeperingen. Een bericht wordt dan in de conceptenbox geplaatst waarna verschillende targets waarmee de inloggegevens worden gedeeld, kunnen inloggen en kennis kunnen nemen van de inhoud van het bericht zonder dat dit ooit als e-mailbericht naar een ontvanger wordt verzonden. Weliswaar bestaat de mogelijkheid om op grond van artikel 17 Wiv 2002 (artikel 39 van het wetsvoorstel) de aanbieder van een communicatiedienst (eerste situatie) of de persoon of instantie die in het kader van de uitoefening van een beroep of bedrijf dergelijke opslag verzorgt (tweede situatie) om de verstrekking van dergelijke gegevens te verzoeken, echter deze zijn niet verplicht om aan een dergelijk verzoek gehoor te geven. Dit achten wij een onwenselijke situatie, zeker nu veel personen en organisaties waar de diensten onderzoek naar verrichten van clouddiensten (in brede zin) 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. Het gebruikmaken van de cloud is inmiddels de normaalste zaak van de wereld; van de 8,5 miljoen smartphones in Nederland maakt een groot gedeelte gebruik van clouddiensten voor e-mail en data-opslag. Dit is ook gebleken bij de targets die de diensten onder meer in kader van contra-terrorisme, contra-inlichtingen en contra-proliferatie in onderzoek hebben. Zij maken op grote schaal gebruik van smartphones en andere moderne digitale voorzieningen zoals de cloud. Om hun intenties en bewegingen in de gaten te houden in het kader van een onderzoek is het gelet op het belang van de nationale veiligheid noodzakelijk dat voor deze onwenselijke situatie een adequate voorziening wordt getroffen. Artikel 54, eerste lid, voorziet daarin. Daarbij wordt opgemerkt dat de tweede situatie strikt genomen niet in de sfeer van onderzoek *van communicatie* ligt, maar omdat het hier evenzeer gaat om toegang tot gegevens die zijn opgeslagen bij een derde (en via een communicatiedienst zijn te benaderen), uit praktische overwegingen (te weten dat daarmee alle clouddiensten worden bestreken) in hetzelfde artikel is opgenomen.

[94] Bij opslagdiensten gaat het om via een netwerk, zoals het internet, beschikbaar stellen van opslagruimte bij een aanbieder, die door de gebruiker op aanvraag kan worden benaderd en waar hij onder meer gegevens kan opslaan (vergelijkbaar met de schijfruimte op de eigen thuiscomputer, maar dan bij een externe partij). Een opslagdienst kan als onderdeel verbonden zijn aan de internettoegangsdienst die bij een aanbieder wordt afgenomen. Verder bieden sommige aanbieders ook de mogelijkheid tot opslag als onderdeel van een pakket clouddiensten. Opslagdiensten kunnen ook sec – al dan niet tegen betaling – worden afgenomen, dus zonder dat deze onderdeel uitmaken van (of gecombineerd zijn met) een bij de aanbieder afgenomen communicatiedienst.

Op grond van artikel 54, eerste lid, van het wetsvoorstel zijn de diensten bevoegd zich te wenden tot: (a) een aanbieder van een communicatiedienst met de opdracht gegevens te 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 en (b) een persoon of instantie die in het kader van de uitoefening van een beroep of bedrijf de opslag verzorgt van door derden via geautomatiseerde werken verwerkte gegevens en waartoe voor die derde rechtstreeks geautomatiseerde toegang bestaat met de opdracht de desbetreffende gegevens te verstrekken. De medewerkingsplicht voor de aanbieder van de communicatiedienst onderscheidenlijk de persoon of instantie die in het kader van de uitoefening van een beroep of bedrijf de opslag verzorgt is in artikel 54, vierde lid, neergelegd.

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 (artikel 54, tweede lid). De toestemming is hier op het niveau van de minister gelegd, aangezien voor zover het hier gaat om gegevens betreffende de inhoud van telecommunicatie daarvoor in het geval dat deze in "stromende" vorm zouden worden verkregen – namelijk door toepassing van de bevoegdheid tot gerichte interceptie ex artikel 47 van het wetsvoorstel – dan wel via het binnendringen in een geautomatiseerd werk van het onderzoekssubject – zie artikel 45 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. Waar het gaat om anderszins opgeslagen gegevens zou voor het geval betrokkene deze op zijn eigen computer zou hebben opgeslagen, voor het verkrijgen van toegang tot de gegevens op die computer op de voet van artikel 45 (binnendringen in een geautomatiseerd werk) toestemming van de minister vereist zijn. Het ligt dan ook in deze situatie voor de hand voor de opslag bij een derde ook het vereiste van ministeriële toestemming te stellen. In beide situaties, zowel artikel 54, eerste lid, onder a, als onder b, van het wetsvoorstel geldt bovendien dat voorafgaand aan de daadwerkelijke uitoefening van de desbetreffende bevoegdheid de verleende toestemming van de minister voor een toets op rechtmatigheid moet worden voorgelegd aan de TIB (zie artikel 36, eerste lid).

Het verzoek om toestemming wordt schriftelijk gedaan en bevat in aanvulling op hetgeen is bepaald in artikel 29, tweede lid, het nummer of een andere aanduiding waarmee de gebruiker als bedoeld in het eerste lid, onder a, onderscheidenlijk de derde als bedoeld in het eerste lid, onder b, 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 54, vijfde lid, is artikel 39, vijfde lid, van overeenkomstige toepassing verklaard. Voor een toelichting ter zake wordt kortheidshalve naar de toelichting op artikel 39 verwezen. In het zesde lid is vervolgens artikel 13.6, tweede en derde lid, Tw van overeenkomstige toepassing verklaard op het voldoen aan een opdracht als bedoeld in het eerste lid. Dat betekent dat degene aan wie de opdracht wordt gericht recht heeft op vergoeding van de door hem in verband daarmee gemaakte administratiekosten en personeelskosten.

Op de gegevens die met toepassing van onderhavige bijzondere bevoegdheid zijn verkregen is artikel 27 (toets op relevantie en vernietiging) van toepassing.

Het opvragen van verkeersgegevens (artikel 55)

In artikel 55 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. Voor de duidelijkheid wordt opgemerkt dat de bevoegdheid geen bewaarplicht inhoudt. 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 3.3.4.4.7.2 van deze memorie van toelichting. Voorts wordt de reikwijdte van de regeling in tweeërlei zin verruimd: (1) voortaan kunnen ook gegevens worden opgevraagd die gerelateerd zijn aan een technisch kenmerk (naast een nummer of een specifieke gebruiker), maar (2) kunnen ook gegevens worden opgevraagd die gerelateerd zijn aan een gespecificeerde locatie (zie het derde lid, onder b). Het gaat bij dit laatste onder meer 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.[95] Voorts 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 87 van het wetsvoorstel opgenomen regeling treedt daarvoor in de plaats.

De diensten zijn op grond van artikel 55, 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. Hieronder valt ook de mogelijkheid dat *real time* locatiegegevens worden verstrekt. De gegevens die door de aanbieder dienen te worden verstrekt zullen, evenals nu het geval is, zich beperken tot die categorieën van gegevens die bij algemene maatregel van bestuur zijn aangewezen. De huidige regeling ter zake, het besluit ex artikel 28 Wiv 2002, zal te zijner tijd aan de nieuwe regeling dienen te worden aangepast.

Het verzoek om toestemming tot uitoefening van de bevoegdheid als bedoeld in het tweede lid, dient te voldoen aan de eisen van artikel 29, tweede lid. De opdracht aan de aanbieder kan pas worden gegeven nadat de toestemming als bedoeld in het tweede lid is verkregen; de opdracht wordt schriftelijk verstrekt en dient de volgende gegevens te bevatten: (a) het nummer dan wel het technische kenmerk 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 55, 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 opdracht als bedoeld in het eerste lid. Voor aanbieders van openbare telecommunicatienetwerken en –diensten als bedoeld in de Telecommunicatiewet is in artikel 13.2a, eerste lid, Tw reeds in een medewerkingsplicht

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

voorzien. Het niet voldoen aan een opdracht tot verstrekking van gegevens is in artikel 143 van het wetsvoorstel strafbaar gesteld.

In artikel 55, 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 opdracht tot gegevensverstrekking als bedoeld in artikel 55, eerste lid.

De verstrekking van gebruikersgegevens (artikel 56)

Artikel 56 geeft een regeling voor het opvragen van gebruikersgegevens[96] bij een aanbieder van een communicatiedienst. Voor de duidelijkheid wordt wederom opgemerkt dat de bevoegdheid geen bewaarplicht inhoudt. De desbetreffende gegevens zijn in het eerste lid limitatief opgesomd. Het betreft gegevens ter zake van (a) naam, adres, postcode, woonplaats, nummer, technisch kenmerk 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.[97] 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 *bitcoins*.

Evenals nu is voor de uitoefening van de bevoegdheid geen toestemming vereist.

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

[96] Vergelijkbaar met abonneegegevens.
[97] Daarnaast is naast nummer – als identificerend gegeven – ook het technisch kenmerk toegevoegd.

stellen 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 56, derde, vierde en zesde lid ter zake van deze andere aanbieders voorzien is in een aanvullende regeling. In het derde lid is de medewerkingsplicht voor deze aanbieders, niet zijnde een aanbieder van openbare telecommunicatienetwerken en –diensten, neergelegd. In het vierde lid is bepaald dat een opdracht tot verstrekking van de gegevens schriftelijk wordt gedaan door of namens het hoofd van de dienst. In het zesde lid is tot slot de in artikel 13.6, tweede en derde lid, Tw opgenomen regeling inzake kostenvergoeding van overeenkomstige toepassing verklaard.

In artikel 56, tweede 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 47 (gerichte interceptie) en artikel 55 (opvragen verkeersgegevens), de aanbieder van een openbare telecommunicatienetwerk of een openbare telecommunicatiedienst als bedoeld in de Telecommunicatiewet op te dragen 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).

3.3.4.4.7.7 Medewerkingsplicht bij ontsleuteling van communicatie

In de artikelen 47, eerste lid, en 48, 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 57 van het wetsvoorstel is de bevoegdheid van de diensten geregeld om in het kader van de uitoefening van de bevoegdheid als bedoeld in de artikelen 47, eerste lid, en 48, 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 de opdracht 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 57, vierde lid, is de medewerkingsplicht neergelegd voor degene tot wie een opdracht als hier bedoeld wordt gericht. Voor de goede orde wordt opgemerkt dat uit de medewerkingsplicht geen bevoegdheid van de diensten kan worden afgeleid tot het (doen) inbouwen van achterdeuren in systemen om aldus toegang tot de ontsleutelde gegevens te krijgen. Ook is er geen enkele verplichting voor bijvoorbeeld aanbieders van communicatiediensten om de encryptie die in hun systemen is toegepast te verzwakken. Voor het uitoefenen van deze bevoegdheid is toestemming van de voor de desbetreffende dienst verantwoordelijke minister vereist (artikel 57, tweede lid). Het verzoek om toestemming is ingevolge het derde lid schriftelijk en dient in aanvulling op hetgeen in artikel 29, tweede 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.

3.3.4.4.8 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 58 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 58 worden thans in relatie tot de bijzondere bevoegdheden waarvoor toegang tot een plaats is vereist de daarmee samenhangende activiteiten omschreven.

De in artikel 58 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. 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 58, derde 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 58, tweede 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 58, derde 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 58, vierde lid, van het wetsvoorstel voorzien in een specifieke regeling ter zake. Aldaar is het eerste tot en met derde 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 58, derde 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 59, vierde lid, van onderhavig wetsvoorstel buiten toepassing verklaard, aangezien in artikel 59, 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 59 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.

3.4 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 59 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.[98] 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.[99] 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[100] en een rapport naar aanleiding van een vervolgonderzoek ter zake bij de AIVD in 2013[101]. Inmiddels heeft de CTIVD op 3 maart 2016 een onderzoek naar notificatie en inzage bij zowel de AIVD als de MIVD aangekondigd. 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.[102] 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.[103] Bij de bespreking van artikel 58 is daar reeds bij stilgestaan. Een volledige afschaffing van de

[98] Kamerstukken II 1999/2000, 25 877, nr. 8, blz. 87-88.
[99] Kamerstukken II 2008/09, 30 977, nr. 18.
[100] CTIVD-rapport nr. 24 (2010).
[101] CTIVD-rapport nr. 34 (2013).
[102] CTIVD-rapport nr. 24 (2010), blz. 27.
[103] Inwerkingtreding per 21 maart 2002 (Stb. 2002, 144).

notificatieplicht – zo die al zou worden overwogen - is gelet daarop dan ook niet mogelijk.

In artikel 59, eerste lid, is de onderzoeksverplichting voor de minister geformuleerd om vijf jaar na beëindiging van de uitoefening van een bijzondere bevoegdheid als bedoeld in de artikelen 44, eerste lid (openen van brieven en andere geadresseerde zendingen), 47, eerste lid (gericht afluisteren), alsmede artikel 58, 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 59, 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. 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 is komen te vervallen. Met de introductie van het nieuwe interceptiestelsel wordt in fase 3, welke in artikel 50 nader is uitgewerkt, namelijk voorzien in een ander stelsel voor de selectie van gegevens in de opbrengst van gegevens die op grond van artikel 48, 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 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 slechts in een enkel geval 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 82, 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 82 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 82 dan ook voor de hand.[104]

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. 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.[105]

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

[104] Zie ook Kamerstukken II 1999/2000, 25 877, nr. 8, blz. 90.
[105] Zie ook Kamerstukken II 2000/2001, 25 877, nr. 14, blz. 57.

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.[106] 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 59, 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 verstrekking van gegevens aan de betrokken persoon, indien deze op het moment van onderzoek een aanvraag als bedoeld in artikel 76 zou hebben ingediend, ingevolge artikel 80 zou moeten worden geweigerd. In het geval het uitbrengen van een verslag dient te worden uitgesteld, herleeft na een jaar de onderzoeksverplichting (artikel 59, eerste lid). Het is echter mogelijk dat uit het onderzoek blijkt dat er sprake is van een afstelgrond als bedoeld in artikel 59, 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 internationale 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

[106] Zie CTIVD-rapport nr. 24, blz. 7 en 8.

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.[107] 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.[108] 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 59, eerste lid, die ten aanzien van de betrokken persoon is uitgeoefend (artikel 59, derde lid, onder b).

Naast de hiervoor besproken uitstel- en afstelgronden voorziet het wetsvoorstel, evenals de huidige wettelijke regeling, in een vervalgrond. In artikel 59, 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

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

RID dan wel een andere relevante bron, worden nagevraagd of deze beschikt over informatie omtrent de verblijfplaats van de betrokkene.[109]

Indien het onderzoek als bedoeld in artikel 59, 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 59, tweede lid, van het wetsvoorstel de CTIVD daarvan met redenen omkleed op de hoogte te worden gesteld.

3.5 Geautomatiseerde (big) data-analyse door de diensten

De diensten zijn op grond van artikel 17 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 slechts voor zover dat noodzakelijk is voor een goede uitvoering van deze wet of de Wet veiligheidsonderzoeken. 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 een effectieve en efficiënte wijze te kunnen verwerken. Bovendien leidt het ontstaan van big data, te weten het fenomeen dat zich onder meer uit in het feit 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 gelet op het heimelijke karakter van de inzet van de

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

bevoegdheden de spanning tussen veiligheid en privacy zich 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.

De Wetenschappelijke Raad voor het Regeringsbeleid (WRR) heeft zich in april 2016 in zijn rapport "big data in een vrije en veilige samenleving" met aanbevelingen gericht aan de overheid in het veiligheidsdomein.[110] De aanbevelingen raken deels aan de eerdergenoemde big data-verwerkingen die plaatsvinden in het kader van de bevoegdheidsuitoefening door de inlichtingen- en veiligheidsdiensten. De Afdeling advisering van de Raad van State heeft in haar advies mede naar aanleiding van het WRR-rapport geadviseerd in te gaan op het belang en de risico's van big data en gevraagd om grotere transparantie bij dit type verwerkingen.

Wat precies onder big data moet worden verstaan, is volgens de WRR niet eenduidig. Voor de duiding van het begrip houdt de WRR een drietal hoofdkenmerken aan, te weten (1) *Data*: het gaat om grote hoeveelheden gestructureerde en ongestructureerde data uit verschillende bronnen; (2) *Analyse*: de analyse is datagedreven, zoekt geautomatiseerd naar correlaties en heeft vooral potentie voor analyses van het heden (*realtime analysis*) en de toekomst (*predictive analysis*). Tot slot moeten de analyses (3) leiden tot *actionable knowledge*, kennis om te kunnen toepassen voor beslissingen op groeps- of individueel niveau. Deze invulling van het begrip big data strookt met de uitgangspunten in de wet.

Zowel de WRR als de Afdeling advisering onderkennen dat big data nuttige en kansrijke toepassingen kent om de veiligheid te bevorderen. Big data heeft een grote potentie omdat tegenwoordig steeds meer data automatisch worden geproduceerd en het onvermijdelijke bijproduct zijn van dagelijkse handelingen van bijna alle burgers, zoals het gebruik van internet, social media, mobiele telefoons en daaraan verbonden applicaties. Daarmee kan het een schat aan informatie opleveren. Big data-verwerkingen door de diensten, zo stellen de WRR en de Afdeling advisering terecht, kan evenwel aan de fundamentele vrijheden van burgers raken. Immers, bij big data-verwerking worden vele grote datasets met gegevens, waarin zich tevens persoonsgegevens kunnen bevinden, benut. De WRR constateert dat de gangbare waarborgen zoals doelbinding en dataminimalisatie echter onvoldoende soelaas bieden om persoonsgegevens te

[110] Met dit rapport geeft de WRR zijn reactie op de adviesaanvraag van het kabinet over het thema "big data, veiligheid en privacy" van 26 mei 2014. Zie Kamerstukken II 2013/14, 26643, nr. 298.

beschermen in big data-verwerkingen. In de optiek van de WRR dienen de waarborgen die nu zien op het verzamelen, te worden uitgebreid naar waarborgen die zien op de analyse en het gebruik van die analyses. Gebruik van profielen die op basis van big data zijn gegenereerd kan leiden tot een "chilling effect" op de grondrechten. De bias die elke dataset in meerdere of mindere mate kenmerkt, kan tot uitkomsten leiden die stelselmatig bepaalde groepen bevoor- of benadelen. Dit effect kan ook afkomstig zijn van de gebruikte algoritmes. De analyses geven immers correlaties en geen causaliteit weer. De uitkomsten zijn dan ook niet onmiddellijk extrapoleerbaar naar individuen. Een correlatie moet altijd worden overwogen, omdat bevindingen anders mogelijk leiden tot stigmatisering en kunnen uitmonden in discriminatie. In het verwerkingsproces en bij de beoordeling van de analyses dient volgens de WRR en de Afdeling advisering aandacht te worden geschonken aan deze risico's. Beiden stellen dat wanneer de overheid op het domein van de veiligheid, waaronder ook de inlichtingen- en veiligheidsdiensten vallen, van big data-verwerkingen wil kunnen profiteren, zowel de data-analyse zelf alsook de besluitvorming of de handeling die daarop vervolgens wordt gebaseerd, met passende waarborgen dient te zijn omkleed. Ten aanzien van de inlichtingen- en veiligheidsdiensten wordt in de hoofdzaak aangedrongen op effectief toezicht door de toezichthouder bij big data-verwerkingen, en strakker reguleren van profielen door onder meer het handhaven van het verbod op geautomatiseerde besluitvorming.

De regering verwelkomt de observaties van de Afdeling advisering van de Raad van State en van de WRR ter zake van de ontwikkelingen in het huidige dynamische technologische tijdgewricht. De regering hecht er in reactie op de adviezen van de WRR en van de Afdeling aan te benadrukken dat aan onder meer de inlichtingen- en veiligheidsdiensten de taak is opgedragen om de burgers te beschermen en hun veiligheid te vergroten opdat zij in vrijheid kunnen leven. De diensten dienen met het oog op het garanderen van die vrijheid zorg dragen voor de maatschappelijke en individuele veiligheid onder meer informatie in te winnen, waakzaam te zijn en bronnen van onveiligheid te bestrijden. Daarbij kan big data van grote waarde zijn. Toepassing van big data kan grote tijdwinst opleveren en tot nauwkeuriger resultaten leiden, waardoor de inlichtingen- en veiligheidsdiensten sneller dan voorheen kunnen inspelen op zeer recente gebeurtenissen, of op gebeurtenissen die mogelijk nog zullen plaatsvinden. Aanslagen kunnen sneller worden gereconstrueerd, hetgeen voorgenomen terroristische voornemens sneller in kaart kan brengen. Ook kan inzet ertoe leiden dat de inzet van de bevoegdheden gerichter kan plaatsvinden, zodat inzet op *bona fide* gebruikers van digitale infrastructuur vaker achterwege kan blijven.

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 op de toegenomen betekenis van verwerkingen met een big data-karakter is het wenselijk om geautomatiseerde data-analyse als werkmethode van de diensten van een expliciete wettelijke grondslag te voorzien. Het voorgestelde artikel 60 strekt daartoe. Voorts wordt daarmee – in combinatie met hetgeen is bepaald in artikel 50, 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 60, 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. Buiten het geval van metadata-analyse, zoals bedoeld in artikel 50, eerste lid, onder b, jo. vierde lid, van het wetsvoorstel wordt – anders dan in de PIA Wiv wordt aanbevolen – niet voorzien in de eis dat de uitoefening van geautomatiseerde data-analyse wordt onderworpen aan ministeriële toestemming. Dat achten wij een te vergaande eis, omdat gegevensverwerking de essentie betreft van het werk van de inlichtingen- en veiligheidsdiensten.

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 de artikelen 17 en 18 van het wetsvoorstel. Zoals uit artikel 60, eerste lid, blijkt, kunnen bij data-analyse ook gegevens uit door derden ter beschikking gestelde gegevensbestanden worden gebruikt. Daarin zitten – net zoals dat ook aan de orde kan zijn bij door de diensten verworven gegevens met toepassing van de in artikel 48 geregelde bevoegdheid tot onderzoeksopdrachtgerichte interceptie - 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 19, vijfde lid, van het wetsvoorstel daartoe een regeling opgenomen.

In artikel 60, tweede lid, is aangegeven dat alle vormen van data-analyse 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 de PIA Wiv wordt er voorts op gewezen dat naast deze (al oude) vormen er andere hedendaagse en voorzienbare toekomstige technische ontwikkelingen zijn, zoals de toepassing van machinaal leren. Voor zover door de diensten nieuwe technieken voor geautomatiseerde data-analyse worden ingezet, zal dat gepaard gaan met een daaraan voorafgaande verkenning van de mogelijkheden die een dergelijke nieuwe techniek biedt, de voor- en nadelen alsmede de mogelijke privacyrisico's. De diensten zijn er goed van doordrongen dat de verwerking van gegevens op een zorgvuldige wijze dient plaats te vinden, omdat dat gevolgen kan hebben voor de personen en organisaties waarop die verwerking betrekking heeft c.q. kan hebben. Nieuwe technieken worden dan ook niet lukraak ingezet, maar eerst getest.

In artikel 60, 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 niet is toegestaan. Aanvankelijk was dit verbod beperkt tot profilering, maar naar aanleiding van het advies van de Afdeling advisering van de Raad van State is besloten het verbod uit te breiden naar alle vormen van geautomatiseerde data-analyse. De resultaten van onderzoeken van inlichtingen- en veiligheidsdiensten kunnen immers een grote impact hebben voor de burgers die in een dergelijk onderzoek worden betrokken. Uitkomsten van geautomatiseerde processen van gegevensverwerking vereisen dan ook menselijke validatie of nadere weging. Het feit dat uit geautomatiseerde data-analyse een bepaald resultaat volgt, dat bovendien ook nog afhankelijk is van de (kwaliteit van de) gehanteerde algoritmen e.d., wil nog niet op voorhand zeggen dat het resultaat juist is (vgl. de mogelijkheid van false positives). Een menselijke afweging van het resultaat in het licht van andere onderzoeksgegevens (en een collegiale toets waar nodig) is juist bij het werk van inlichtingen- en veiligheidsdiensten van het grootste belang; het is immers geen mathematische aangelegenheid maar juist een activiteit waarbij bij voortduring sprake is van weging, inschatting, interpretatie van onderzoeksresultaten in combinatie met elkaar en in het licht van de specifieke onderzoeksvraag. Er is in casu dus altijd menselijke tussenkomst vereist. Daarmee wordt ook aangesloten bij de aanbeveling van de WRR in eerder genoemd rapport dat, gelet op het risico van stigmatisering en mogelijke discriminatie van individuen of groepen personen als gevolg van geautomatiseerde besluitvorming het noodzakelijk is om te voorzien in menselijke tussenkomst bij analyse-uitkomsten die

gevolgen hebben voor individuen of groepen burgers. Aldus wordt voldaan aan het advies van zowel de WRR als de Afdeling advisering om het verbod van automatische besluitvorming in te kaderen. Bovendien heeft de onafhankelijke toezichthouder toegang tot gegevensverwerkingsprocessen gedurende de gehele verwerkingscyclus, en kan deze beoordelen of op juiste wijze invulling wordt gegeven aan het verbod, zoals vastgelegd in artikel 60, derde lid, van het wetsvoorstel.

De WRR beveelt daarnaast aan om big data-toepassingen in het veiligheidsdomein onderwerp te laten zijn van een externe 'review', die in het bijzonder toeziet op de gemaakte keuzes inzake data en methode van analyse. Bij dit toezicht dient tevens te worden getoetst of de datasets up-to-date zijn en of de algoritmes en methoden die bij de data-analyse worden gebruikt deugdelijk zijn en voldoen aan wetenschappelijke criteria voor statistisch onderzoek. Het belang van het uitvoeren van '*reviews'*, waaronder wij begrijpen het toetsen van de gemaakte keuzes inzake data en methode van analyse aan algemene juridische en kwaliteitseisen, wordt door de regering onderschreven. In dit verband wenst de regering op te merken dat met het voorgestelde stelsel van toestemmingverlening en van het toezicht door de CTIVD tijdens de uitvoering van de bijzondere bevoegdheden wordt voldaan aan deze aanbeveling. De capaciteit van de CTIVD zal worden uitgebreid. Daarbij ontstaat ruimte om experts op het terrein van data-analyses te betrekken.

De Afdeling advisering adviseerde - in lijn met het WRR-rapport – om transparantie in de big data- verwerkingsprocessen door de overheid te vergroten teneinde het vertrouwen van de samenleving in de zorgvuldigheid en proportionaliteit van big data gegevensverwerking te behouden. Hoewel het noodzakelijk heimelijke karakter van de gegevensverwerking - inclusief big data- in het kader van de uitvoering van de taken van de Wiv ertoe leidt dat de regering het uitgangspunt hanteert dat er geen volledige transparantie kan bestaan jegens eenieder voor wat betreft inzage in de gehanteerde werkmethoden van de diensten, wil zij benadrukken dat wel zij graag nadere invulling wil geven aan het advies met betrekking tot transparantie omdat zij het belang van het behoud van het vertrouwen van de samenleving in de big data-verwerking door de diensten onderschrijft. Teneinde de transparantie over de big data-verwerkingen te vergroten zet de regering in op het robuuster maken van twee instrumenten, te weten het Jaarplan van de AIVD en van de MIVD en capacitaire uitbreiding van het onafhankelijke toezicht. Het Jaarplan van de AIVD en van de MIVD zal met het oog daarop worden aangevuld met een paragraaf over het gebruik van big data, waarbij specifiek aandacht wordt besteed aan de *doelen* en *frequentie* van het gebruik van big data en de mate waarin deze hebben bijgedragen aan het boeken van resultaten en het

ontdekken van trends. Daarnaast zal worden beschreven of mitigerende maatregelen getroffen moesten worden om afwijkingen in de gegevensbronnen en analyses te corrigeren, teneinde een zinvolle analyse en daaruit voortvloeiende besluitvorming tot stand te kunnen brengen. Het Jaarplan van de AIVD en van de MIVD is vanwege zijn inhoud staatsgeheim en wordt integraal gedeeld met de Commissie voor de Inlichtingen- en veiligheidsdiensten. Wel wordt deze op hoofdlijnen openbaar gemaakt en aan het parlement aangeboden. De hoofdlijnen kunnen onder de aandacht van burgers worden gebracht op de website van de AIVD en de MIVD.[111]

3.6 De verstrekking van gegevens

3.6.1 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 diverse onderdelen is zij echter aangepast. Allereerst wordt in artikel 63 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. Ten tweede is ten opzichte van de huidige wet een nieuw artikel (artikel 64) opgenomen dat de mogelijkheid biedt voor de diensten om in het kader van een goede taakuitvoering ongeëvalueerde gegevens te verstrekken aan buitenlandse collegadiensten. 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. Een vierde aanpassing betreft een aanvulling van de regeling inzake het doen van mededelingen aan het openbaar ministerie met voorafgaande rechterlijke toets voor zover de mededeling betrekking heeft op gegevens die betrekking hebben op de vertrouwelijke communicatie tussen een advocaat en diens cliënt. Tot slot wordt nadrukkelijk bepaald dat bij het doen van mededelingen aan het openbaar ministerie (artikel 66) en ingeval van een dringende of gewichtige reden (artikel 67) een dergelijke mededeling niet alleen uit eigen beweging, maar ook desgevraagd kan plaatsvinden.

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 62, derde lid). Dit is wenselijk gelet op het bijzondere karakter van de gegevens die door of ten behoeve van de diensten worden

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

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 66 en 67 (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 collegadiensten van andere landen (artikelen 86 en 89 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.

3.6.2 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 61 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 91 onderscheidenlijk 92, voor zover zij – binnen het kader van genoemde artikelen – werkzaamheden verrichten voor de AIVD onderscheidenlijk de MIVD. Ingevolge artikel 61 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.

3.6.3 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[112]; maar

[112] 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

ook kan het bijvoorbeeld gaan om ten behoeve van zogeheten belangendragers opgestelde specifieke analyses gaan.[113] 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 68 tot en met 70). 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 18 van het wetsvoorstel.

3.6.3.1 Algemene bepalingen

Artikel 62: mededeling in het kader van een goede taakuitvoering van de diensten

In artikel 62 wordt een (algemene) regeling gegeven voor het *in het kader van een goede taakuitvoering* doen van een mededeling omtrent door of ten behoeve van de dienst verwerkte gegevens. Dit artikel is ten opzicht van het huidige artikel 36 ongewijzigd gebleven. De bevoegdheid tot het doen van een mededeling is daarbij in algemene zin in handen gelegd bij de diensten, zij het dat er situaties kunnen voordoen waarbij de mededeling gelet de aard daarvan dient plaats te vinden door de voor de dienst verantwoordelijke minister (zie artikel 62, tweede lid). Dit zal met name dan aan de orde zijn, wanneer er bijvoorbeeld grote politieke risico's aan de mededeling van de desbetreffende gegevens zijn verbonden.

Evenals nu wordt in artikel 62 gesproken over het doen van een *mededeling* omtrent door of ten behoeve van de dienst verwerkte gegevens.[114] Hoewel de mededeling als zodanig ook als een vorm van 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

---

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).

[113] 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.

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

artikel 23 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 66, vierde lid, 67, tweede lid, 68, derde lid en 69, vierde lid, van het wetsvoorstel. Waar het gaat om mededelingen aan het openbaar ministerie (artikel 66) dient de inzage desgevraagd te worden verleend; in de andere gevallen bestaat ter zake een discretionaire bevoegdheid.

In artikel 62, 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-, verbindingsinlichtingen- en inlichtingenorganen. Bij de in laatste categorie genoemde internationale beveiligings-, verbindingsinlichtingen- en inlichtingenorganen moet worden gedacht aan de NAVO, EU of VN.

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.

Artikel 63: mededeling in het kader van een 'naslag'

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 63 van het wetsvoorstel wordt een nadere regeling gegeven voor de mededeling van gegevens in dit kader alsmede

voor het daaraan ten grondslag liggende verzoek. Deze regeling ziet op een specifieke categorie van mededelingen die plaatsvindt in het kader van een goede taakuitvoering van de diensten. In artikel 63, 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 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 63, 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[115], 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 63, derde lid, biedt hiervoor de mogelijkheid. In artikel 63, 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 64: verstrekking van ongeëvalueerde gegevens aan buitenlandse diensten

[115] 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.

In artikel 64 wordt voorzien in de mogelijkheid dat de diensten *in het kader van de (eigen) goede taakuitvoering* ongeëvalueerde gegevens kunnen verstrekken aan buitenlandse collegadiensten. Deze verstrekkingsmogelijkheid dient te worden onderscheiden van de mogelijkheid tot verstrekking van ongeëvalueerde gegevens op grond van artikel 89 van het wetsvoorstel. Hier gaat het om een verstrekking waartoe *een eigen goede taakuitvoering van de AIVD of de MIVD noodzaakt*; bij de verstrekking op grond van artikel 89 vindt de verstrekking (primair) plaats in het kader van een samenwerkingsrelatie ten behoeve van door die buitenlandse dienst te behartigen belangen. Anders dan bij artikel 89 hoeft bij een verstrekking op grond van artikel 62, eerste lid, aanhef en onder d, als bij een verstrekking op grond van artikel 64, geen samenwerkingsrelatie te bestaan, waarvoor eerst een weging als bedoeld in artikel 88 van het wetsvoorstel heeft plaatsgevonden. Waar het gaat om geëvalueerde gegevens (artikel 62) is de wenselijkheid om daaromtrent mededeling te kunnen doen, in het bijzonder ingegeven om bijvoorbeeld ingeval de diensten de beschikking krijgen over gegevens die wijzen op een terroristische aanslag in een land waar met de desbetreffende inlichtingen- of veiligheidsdienst (nog) geen samenwerkingsrelatie bestaat deze gegevens toch te kunnen verstrekken.

Omdat niet valt uit te sluiten dat er zich in de toekomst een situatie voordoet waardoor een acute noodzaak ontstaat om ook ongeëvalueerde gegevens te verstrekken aan een land waarmee geen samenwerkingsrelatie bestaat, is de voorziening in artikel 64 getroffen.

Een dergelijke verstrekking zal zich uitsluitend in uitzonderingssituaties kunnen voordoen. Alleen indien dringende en gewichtige redenen daartoe noodzaken. Voorts kan van verstrekking pas sprake zijn indien de betrokken minister hiermee zelf heeft ingestemd. Dit is in artikel 64 tot uitdrukking gebracht.

Artikel 65: de derde partij-regel

In artikel 65, 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 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 65, tweede lid, is bepaald dat de derde partij-regel altijd moet worden gesteld bij verstrekking van gegevens aan buitenlandse collegadiensten als bedoeld in artikel 62, eerste lid, onder d. In artikel 88, derde lid, van het wetsvoorstel is (onder meer) artikel 65 van overeenkomstige toepassing verklaard, waar het gaat om gegevensverstrekking aan buitenlandse collegadiensten als bedoeld in artikel 89, eerste lid.

Het niet zonder voorafgaande toestemming verder verstrekken van gegevens 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 waaronder de kring van gerechtigden om van de gegevens kennis te nemen – geheim worden gehouden. Het is evident dat mede gelet op het feit dat het internationale karakter van dreigingen eerder toe- dan af zal nemen, samenwerking tussen diensten van essentieel belang is om de benodigde informatiepositie te verwerven en te behouden en op een adequate manier samen te kunnen reageren op dreigingen.

In artikel 65, derde lid, is ten slotte de mogelijkheid geopend dat in de gevallen dat gegevens onder toepassing van de derde partij-regel 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 wanneer een buitenlandse collegadienst onderkent dat er in het belang van een tijdige en efficiënte reactie op een dreiging nog een collegadienst moet worden ingelicht, toestemming worden verleend om gegevens verder te verstrekken. Wel kunnen aan die toestemming voorwaarden worden verbonden, zoals over de aard en het doel van het gebruik.

Artikel 66: ambtsberichten aan het openbaar ministerie

Artikel 66 van het wetsvoorstel geeft een regeling voor het doen van een mededeling van door of ten behoeve van een dienst 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, zij het dat in het voorgestelde artikel 66, eerste lid, thans is geëxpliciteerd dat deze mededeling ook desgevraagd aan het openbaar ministerie kan plaatsvinden. 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 66, 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 gedaan; 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.[116] 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.[117] 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 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 desbetreffende minister en de Minister van Veiligheid en Justitie gezamenlijk hem daartoe schriftelijk van de verplichting tot geheimhouding hebben ontheven (zie artikel 86, tweede lid, Wiv 2002; artikel 136, tweede lid, van het wetsvoorstel). Om de hiervoor geconstateerde spanning weg te

[116] Zie ook Kamerstukken II 1997/98, 25 877, nr. 3, blz. 58.
[117] 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.

nemen is dan ook in voorliggend wetsvoorstel ervan afgezien de zinsnede "onverminderd dat daartoe een wettelijke verplichting bestaat" opnieuw op te nemen.[118]

Een mededeling als bedoeld in artikel 66, 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 66, 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 66, 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 135 en 136 van het wetsvoorstel, waarin specifieke geheimhoudingsverplichtingen zijn neergelegd, zijn daarbij van 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.

In artikel 66, derde lid, van het wetsvoorstel is ten slotte ten opzichte van de bestaande regeling een nieuw onderdeel opgenomen dat betrekking heeft op het geval dat de diensten in het kader van hun goede taakuitvoering stuiten op gegevens die betrekking hebben op de vertrouwelijke communicatie tussen een advocaat en een cliënt en waarvan men van mening is dat daarvan mededeling dien te worden gedaan aan het openbaar ministerie. Het betreft hier een uitermate delicate problematiek, mede in het

[118] 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.

licht van de beperkingen die in het kader van strafvordering zijn gesteld aan de verwerving en het gebruik van dergelijke communicatie. Deze regeling is opgenomen naar aanleiding van de uitspraak van de voorzieningenrechter rechtbank Den Haag van 1 juli 2015 (bevestigd door het gerechtshof Den Haag in haar uitspraak van 27 oktober 2015)[119], waarbij deze met ingang van 1 juli 2015 de Staat heeft verboden om opbrengsten verkregen uit de inzet van bijzondere bevoegdheden waarbij communicatie van en met advocaten is afgeluisterd aan het openbaar ministerie te verstrekken, zonder dat voorafgaand aan die verstrekking een onafhankelijke toets heeft plaatsgevonden met betrekking tot de rechtmatigheid van die verstrekking, bij welke toetsing beoordeeld dient te worden of de informatie onder het verschoningsrecht valt en zo ja, onder welke voorwaarden deze mag worden verstrekt. In de voorgestelde regeling wordt deze onafhankelijke toets in handen gelegd van de rechtbank Den Haag, die voor het mogen doen van een dergelijke mededeling door de diensten aan het openbaar ministerie toestemming dient te verlenen. Indien de rechtbank de toestemming niet verleent, dient de mededeling achterwege te blijven. In artikel 66, derde lid, laatste volzin, is het tweede lid van artikel 66 buiten toepassing verklaard; er bestaat dus geen mogelijkheid om in spoedeisende gevallen de mededeling mondeling te laten geschieden. Vooruitlopend op de totstandkoming van een wettelijke regeling, zoals met betrekking tot artikel 66, derde lid, is voorgesteld, is er een tijdelijke voorziening getroffen; zie daartoe artikel 8 van de Tijdelijke regeling onafhankelijke toetsing bijzondere bevoegdheden Wiv 2002 jegens advocaten en journalisten (Stcrt. 2015, nr. 46477).

Artikel 67: mededeling op grond van een dringende en gewichtige reden

Artikel 67, 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. Evenals bij de regeling van het doen van een mededeling aan het openbaar ministerie wordt hier ten opzichte van de bestaande regeling geëxpliciteerd dat een dergelijk mededeling ook desgevraagd kan plaatsvinden. Het gaat in deze gevallen om een mededeling die plaatsvindt anders dan in het kader van de uitvoering van de aan de diensten in artikel 8 en 10 opgedragen taken. Bij deze mededeling 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 mededeling niet mogelijk zijn.

[119] ECLI:NL:RBDHA:2015:7436 en ECLI:NL:GHDHA:2015:2881

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 mededeling 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 67, tweede lid, is artikel 68, tweede en derde lid, van overeenkomstige toepassing verklaard. Kortheidshalve wordt verwezen naar hetgeen verderop in de toelichting daaromtrent is opgemerkt.

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.

3.6.3.2 Bijzondere bepalingen betreffende de externe verstrekking van persoonsgegevens

In paragraaf 3.4.2.2 (artikelen 68 tot en met 70) 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[120], 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 68 van het wetsvoorstel enkele waarborgen opgenomen met betrekking tot de mededeling 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 68, eerste lid, in dergelijke gevallen

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

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 68, derde lid, is tot slot een grotendeels met artikel 66, vierde 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 66, vierde 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 135 en 136, tweede en derde lid, van overeenkomstige toepassing. Anders dan bij artikel 66, is artikel 136, eerste lid, hier niet van overeenkomstige toepassing verklaard; dat 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 136, eerste lid, kan deze dan de LOvJ van diens geheimhoudingsverplichting tegenover hem ontslaan.

Artikel 69 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 mededeling van de hiervoor bedoelde persoonsgegevens wel dient plaats te vinden. In artikel 69, tweede lid, is daarbij voor een drietal situaties de mogelijkheid geschapen. In artikel 69, tweede lid, aanhef en onder a, is allereerst bepaald dat in afwijking van het eerste lid mededeling 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 collegadienst kan bevinden. De omtrent hem beschikbare informatie bij de AIVD of MIVD kan in voorkomende gevallen voor die buitenlandse collegadienst van belang zijn bij het onderzoek dat door die collegadienst 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 77, 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 69, 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 68, derde lid. Zoals reeds eerder is aangegeven, biedt dat artikel de mogelijkheid 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 70 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 20, tweede lid, verplicht daartoe.

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 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 28), de toestemmingsduur en de inhoud van een verzoek om toestemming (artikel 29) alsmede de bepaling betreffende de verslaglegging van de uitoefening van de bevoegdheid (artikel 31). Artikel 71 voorziet daarin.

In de artikelen 72 en 73 is de bevoegdheid tot het verlenen van toestemming voor de uitoefening van de bijzondere bevoegdheid in handen gelegd van de voor de dienst verantwoordelijke minister of namens deze het hoofd van de desbetreffende dienst. Het hoofd van een dienst kan aan hem ondergeschikte ambtenaren bij schriftelijk besluit aanwijzen die de toestemming, bedoeld in de tweede volzin, namens hem verlenen.

4.2 De oprichting en inzet van rechtspersonen

In artikel 72 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 (met de mogelijkheid van ondermandaat). Nieuw is verder het bepaalde in artikel 72, derde 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 artikel 26 van het wetsvoorstel van overeenkomstige toepassing te verklaren. De daarin neergelegde proportionaliteits- en subsidiariteitstoets is in casu niet aan de orde. Tot slot wordt opgemerkt dat één en dezelfde rechtspersoon ook voor meerdere onderzoek tegelijk kan worden ingezet. In dat geval zal wel per onderzoek toestemming dienen te worden verkregen.

4.3 Het bevorderen of treffen van maatregelen

In artikel 73 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 in het huidige 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 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 73 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[121]. Bezien is op welke wijze dit het beste geïmplementeerd kan worden. Voor een deel kan dit plaats vinden door in artikel 73 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 73, derde lid, geeft daaraan invulling. Aldaar wordt bepaald dat bij het bevorderen of treffen van een maatregel slechts die maatregel wordt

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

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 betrokkene – jegens wie de maatregel wordt bevorderd of getroffen – de minste nadeel oplevert. Voorts is artikel 26, tweede tot en met vierde lid, van overeenkomstige toepassing verklaard. Ingevolge artikel 26, tweede 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 26, derde lid, bepaalt aansluitend dat de uitoefening van de bevoegdheid evenredig dient te zijn aan het daarmee beoogde doel. Op grond van artikel 26, vierde lid, 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 73 aangegeven lijnen - het bij de toepassing van deze bijzondere bevoegdheid te hanteren afwegingskader nader worden geoperationaliseerd.

In artikel 73, vierde lid, is bepaald dat het bevorderen of treffen van maatregelen bij instructie kan worden opgedragen aan een natuurlijke persoon als bedoeld in artikel 41, 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 41, eerste lid, dient te geschieden, voorziet artikel 41, 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 41, 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 41, vierde tot en met zevende lid, opgenomen kader ook in deze gevallen van overeenkomstige toepassing te worden verklaard. Artikel 73, vijfde lid, voorziet daarin, zij het dat naast de agent als bedoeld in artikel 41 uitsluitend medewerkers van de dienst mogen worden belast met het (mede)plegen van strafbare feiten, waarbij tevens is bepaald dat onder “natuurlijke persoon” of “persoon” in de genoemde artikelleden dient te worden verstaan: de medewerker van de dienst die wordt belast met het bevorderen of treffen van maatregelen als bedoeld in het eerste lid. Aldus wordt bewerkstelligd dat met inachtneming van de in artikel 41, vierde tot en met zevende lid, opgenomen bepalingen, ook deze medewerkers 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.[122] 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.[123]

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 74 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

[122] Rapport van de Commissie Dessens, *Evaluatie Wet op de inlichtingen- en veiligheidsdiensten 2002. Naar een nieuwe balans tussen bevoegdheden en waarborgen*, par. 7.2.7 (blz. 141).
[123] Kamerstukken II 2013/14, 33 820, nr. 2, blz. 7-8.

Wob, waaronder de uitleg van enkele begrippen (artikel 75 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 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 76, 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 79, 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.[124] 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.[125] 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

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

In artikel 76 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 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.[126] 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.[127] 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 81) 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 76, 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 79, eerste lid, van het wetsvoorstel (huidig artikel 50, eerste lid), is in verband daarmee bepaald dat artikel 76 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 79, tweede lid, worden enkele minimumeisen aan de inhoud van de aanvraag gesteld, waarmee op een zo eenduidig mogelijke manier kan worden vastgesteld op

[126] 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.
[127] Zie hetgeen daaromtrent onder meer is gesteld in Kamerstukken II 1997/98, 25 877, nr. 3, blz. 64.

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 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 79, 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 76 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 81) 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[128]), 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 81, 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.

[128] Ingevolge artikel 7, tweede lid, van de Wet openbaarheid van bestuur 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.

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 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 76 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.[129]

Zoals indertijd ter toelichting op de in artikel 48 Wiv 2002 (het thans voorgestelde artikel 77) is gesteld[130], 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 69, tweede lid, van het wetsvoorstel toch nog worden verstrekt, ingevolge het bepaalde in artikel 69, 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

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

gegeven te verbeteren onderscheidenlijk te verwijderen (zie artikel 20 van het wetsvoorstel).

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

Het wetsvoorstel voorziet, evenals nu, in een van artikel 76 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 76 en 79 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.[131] 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 78, 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 78, 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

[131] Waar het gaat om de ambtenaren, bedoeld in de artikelen 91 en 92, 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.

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 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 78, derde lid, biedt daartoe aldus de mogelijkheid. Tegen dit besluit staat bezwaar en beroep open. Anders dan bij inzage op grond van artikel 76 of artikel 79 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 78, zesde lid, artikel 85 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 80) van het wetsvoorstel is het recht op kennisneming van andere gegevens dan persoonsgegevens opgenomen. Op grond van artikel 80, 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 75 wordt onder bestuurlijke aangelegenheid hier hetzelfde verstaan als in de Wet openbaarheid van bestuur (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 82 tot en met 85) 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 Wiv 2002) 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. [132]

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.[133] 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.[134] 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

[132] Zie onder meer Kamerstukken II 1997/98, 25 877, nr. 3, blz. 68-71.
[133] Zie EHRM 6 september 1978, *Klass e.a. t. Duitsland*, par. 58.
[134] Kamerstukken II 1997/98, 25 877, nr. 3, blz. 69.

verwerkt door de diensten, maar waarvan de wetenschap daarover voor de huidige taakuitvoering van de diensten niet langer meer relevant is. Dergelijke gegevens kunnen 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[135], die thans in artikel 80 van het wetsvoorstel (huidig artikel 53 Wiv 2020) is neergelegd. Met deze weigeringsgrond wordt het toetsingscriterium "actueel kennisniveau" op wetsniveau nader uitgewerkt. Nu artikel 82 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 84, 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.[136] In beide gevallen dient dus een weigering van het verzoek mogelijk te zijn.

In artikel 82 van het wetsvoorstel is dit – in navolging van artikel 53 van de Wiv 2002 – als volgt uitgewerkt. Een aanvraag als bedoeld in artikel 76 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

[135] Artikel 83 verklaart artikel 82 van overeenkomstige toepassing op een aanvraag als bedoeld in artikel 79.
[136] Zie ook Kamerstukken II 2000/01, 25 877, nr. 14, blz. 75.

uitgangspunt heeft als bijkomend voordeel dat de bestuurlijke lasten voor de behandeling 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.[137]

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 82, eerste lid, onderdeel b, zijn uitwerking gekregen. Ingevolge artikel 82, 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 83 is de regeling van artikel 82 ook van toepassing verklaard op verzoeken om kennisneming van door of ten behoeve van de diensten verwerkte persoonsgegevens als bedoeld in artikel 79 van het wetsvoorstel.

In artikel 84, 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 80 (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 82 of 83 (artikel 84, vierde lid). De hier opgenomen weigeringsgronden komen vrijwel geheel

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

overeen met de weigeringsgronden in artikel 10, eerste en tweede lid, Wob.[138] 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 84, 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 80, maar ingevolge artikel 84, vierde lid, ook voor aanvragen als bedoeld in artikel 76 onderscheidenlijk 79. 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 85 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 Nationale Politie, het Openbaar Ministerie (OM), de Rijksbelastingdienst, de Immigratie en Naturalisatiedienst (IND) en de Koninklijke Marechaussee (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 de Algemene Inlichtingen- en Veiligheidsdienst en de Militaire Inlichtingen- en Veiligheidsdienst

In de artikelen 86 en 87 wordt het wettelijk kader gegeven voor de samenwerking tussen de AIVD en de MIVD. Artikel 86 van het wetsvoorstel sluit aan bij hetgeen thans in artikel 58 van de huidige wet is geregeld, zij het dat, overeenkomstig de aanbeveling

[138] Het begrip veiligheid van de staat is in artikel 84, eerste lid, onder b, vervangen door nationale veiligheid; zie ook het huidige artikel 55, eerste lid, onder b, Wiv 2002.

van de Commissie Dessens, de regeling van samenwerking tussen de diensten verder gaat dan de huidige plicht om elkaar zoveel mogelijk medewerking te *verlenen* en aan de diensten wordt opgedragen zoveel mogelijk *samen te werken* (artikel 86, eerste lid). Daarmee wordt ook uitdrukking gegeven aan een ontwikkeling die heeft plaatsgevonden in de afgelopen jaren, waarbij in toenemende mate in gezamenlijk werkverbanden (gemeenschappelijk teams) en op operationeel gebied wordt samengewerkt. Met het nieuwe artikel 86, vierde lid, waarop hierna nog afzonderlijk wordt ingegaan, wordt beoogd dat proces te faciliteren.

Artikel 86, 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. Naar aanleiding van een aanbeveling in de PIA Wiv is de bepaling thans geformuleerd als bevoegdheid. Een en ander heeft tot gevolg dat een aantal algemene beginselen van gegevensverwerking (thans nadrukkelijk) ook op de gegevensverstrekking van toepassing zijn. Gewezen wordt op de algemene bepalingen inzake gegevensverwerking in paragraaf 3.1 van het wetsvoorstel. In artikel 86, derde lid, is de procedure die bij verzoeken om technische en andere vormen van ondersteuning moet worden gevolgd uitgewerkt, voor zover deze betrekking hebben op de uitoefening van bijzondere bevoegdheden als bedoeld in paragraaf 3.2.5 (gericht op gegevensverwerking), 4.2 of 4.3 (overige bijzondere bevoegdheden). 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. Ten opzichte van de huidige situatie bevat het derde lid een beperkte wijziging. In het derde lid is verwoord dat de verzochte ondersteuning slechts wordt verleend indien daarvoor toestemming is verkregen van de voor ondersteunende dienst verantwoordelijke minister of namens deze het hoofd van die dienst.

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 86, vierde lid, wordt beoogd hiervoor de nodige ruimte te bieden, echter zonder dat de bestaande verantwoordelijkheidsverdeling wordt aangetast. Immers te allen tijde 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 86, 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.[139] Met de in het vierde lid voorgestelde regeling wordt aan dergelijke samenwerkingsverbanden een expliciete wettelijke grondslag gegeven, die ook deel uit gaat maken van het wettelijk kader waarover het rechtmatigheidstoezicht van de CTIVD zich uitstrekt. Overigens wordt opgemerkt dat 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 tevens afspraken worden gemaakt over de ondersteuning bij de uitoefening van bijzondere bevoegdheden, waarbij echter niet afgeweken kan worden van het bepaalde in artikel 86, derde lid, van het wetsvoorstel. 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 86, 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.

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

Artikel 87 van het wetsvoorstel biedt ten opzichte van de huidige wet een nieuwe regeling, waarbij, onder verwijzing naar de samenwerking in artikel 86, 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 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 87 te vervallen.[140] 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 87 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 87. 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 samen met een veelheid van buitenlandse diensten. Deze samenwerking heeft door de internationale ontwikkelingen op veiligheidsgebied, vergelijk de situatie in het Midden Oosten en Noord-Afrika, alleen

[140] 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.

maar aan belang en intensiteit gewonnen. In de jaarverslagen van beide diensten over 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 de praktijk van samenwerking van inlichtingen- en veiligheidsdiensten is immers bij de uitwisseling van informatie het beginsel van 'quid pro quo' (voor wat hoort wat) een belangrijk element. Overigens is ook de *need to share* een belangrijk beginsel. Bijvoorbeeld binnen het verband van de Counter Terrorism Group (CTG) speelt 'quid pro quo' een beperktere rol omdat in de samenwerking tussen de Europese diensten informatie, die betrekking heeft op terrorisme dreigingen jegens een van de aangesloten landen, verwacht wordt te worden verstrekt zonder dat er iets voor wordt terugverwacht. Ook bij militaire operaties is het delen van informatie cruciaal. Aldus kan gefragmenteerde informatie worden gecompleteerd. Zonder de uitwisseling van gegevens zal mogelijk geen van de partijen ooit het benodigde inzicht verkrijgen. De CTIVD heeft in een aantal toezichtsrapporten aandacht besteed aan (diverse aspecten van) de samenwerking van de AIVD en de MIVD met buitenlandse collegadiensten[141]; een vervolgonderzoek naar de samenwerking van de AIVD met buitenlandse inlichtingen- en veiligheidsdiensten (onderzoek "gegevensuitwisseling (vermeende) jihadisten") vindt thans plaats.[142] Recent zijn de onderzoeksrapporten inzake het onderzoek naar de uitvoering van Tweede Kamermoties nrs. 89 en 96 aan het parlement aangeboden.[143] 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 88 de bevoegdheid tot het aangaan van samenwerkingsrelaties met buitenlandse collegadiensten geregeld alsmede de daaraan voorafgaande, door de diensten te maken, weging die bepalend is voor de vraag of en, zo ja, waaruit die samenwerking kan bestaan. In artikel 89 wordt vervolgens een

[141] 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 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 en het meer recente rapport 22b over samenwerking van de MIVD met buitenlandse inlichtingen- en veiligheidsdiensten.

[142] Aangekondigd door de CTIVD op 10 maart 2016.

[143] CTIVD-rapport nr. 48 (2016) over de invulling van de samenwerkingscriteria door de AIVD en de MIVD, alsmede CTIVD-rapport nr. 49 (2016) over de uitwisseling van ongeëvalueerde gegevens door de AIVD en de MIVD. Beide rapporten zijn door de minister van BKZ en de minister van Defensie op 30 juni 2016 aan het parlement aangeboden.

regeling gegeven voor de verstrekking van gegevens alsmede het verlenen van technische en andere vormen van ondersteuning *aan* buitenlandse collegadiensten. Artikel 90 geeft tot slot een regeling voor het doen van verzoeken om technische en andere vormen van ondersteuning aan buitenlandse collegadiensten *door* de AIVD of MIVD. Een regeling voor dit laatste ontbreekt in de huidige wet.

6.3.2 Het aangaan 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 JSCU treedt het hoofd van deze gemeenschappelijk eenheid als point of contact (POC) 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 plaatsvindt. De betrokken minister dient over de samenwerking te worden geïnformeerd en bij risicovolle collegadiensten dient de besluitvorming aan de minister te worden voorgelegd. Voorafgaand aan het aangaan van een samenwerkingsrelatie met een buitenlandse inlichtingen- of veiligheidsdienst wordt een aantal zaken onderzocht.[144] 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[145] 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 de rapporten 22a (2009) en 22b (2015) aan deze alsmede enkele andere criteria.[146] 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 Amerikaanse National Security Agency (NSA), nader

[144] Kamerstukken II 2000/01, 25 877, nr. 59, p. 16 en Aanhangsel Handelingen II 2004/05, nr. 749.
[145] Zo is Nederland partij bij verdragen op het vlak terrorismebestrijding, hetgeen tot samenwerking – ook tussen inlichtingen- en veiligheidsdiensten – noopt.
[146] 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').

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

In het voorgestelde artikel 88 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 88, 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 om te bepalen 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 collegadienst 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 collegadienst 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) collegadiensten 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 collegadienst 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 de rapporten 22a en 22b dienen de diensten 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.[147] 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 collegadienst – 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 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 aan de samenwerking zijn verbonden wordt van oudsher terughoudendheid betracht bij het uitwisselen van persoonsgegevens. Uitgangspunt blijft dat op voorhand geen enkele 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 88, 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 88, 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

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

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 87, 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 88 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[148] – aan een buitenlandse dienst gegevens te verstrekken dan wel daaraan technische of andere vormen van ondersteuning te verlenen. Deze regeling is in artikel 89 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 onvoldoende wettelijk geregeld. Op beide regelingen zal thans nader worden ingegaan.

Artikel 89, eerste lid, bepaalt dat in het kader van een samenwerkingsrelatie als bedoeld in artikel 88 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 collegadienst, zoals die in het kader van artikel 88 is vastgesteld, medebepalend zal zijn. Op de verstrekking van gegevens zijn in artikel 89, derde lid, de artikelen 65, 69 en 70 van overeenkomstige toepassing verklaard. De verstrekking van gegevens in het kader van het eerste lid kan zowel

[148] In dat geval vindt de gegevensverstrekking plaats op basis van artikel 36, eerste lid, onder d, Wiv 2002 (artikel 62, eerste lid, onder d, van het wetsvoorstel; voor zover het betrekking heeft op ongeëvalueerde gegevens geeft artikel 64 daarvoor een regeling).

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 uitwisseling van ongeëvalueerde gegevens[149] met buitenlandse diensten zal worden onderworpen aan een systeem van ministeriële toestemming.[150] In artikel 89, tweede lid, wordt daarin voorzien. Wat hier onder ongeëvalueerde gegevens moet worden begrepen is bijvoorbeeld de in het kader van artikel 48 ontvangen en opgenomen gegevens waarop nog geen selectie is toegepast als bedoeld in artikel 50, 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. Dat is met name van belang voor de uitwisseling van dergelijke gegevens in het kader van specifieke internationale samenwerkingsverbanden.

Tijdens de internetconsultatie en in de PIA Wiv zijn er vragen gesteld met betrekking tot de gegevensuitwisseling met buitenlandse diensten. Benadrukt wordt dat intensieve internationale samenwerking, en daarmee ook de uitwisseling van ongeëvalueerde gegevens, onmisbaar is. Zoals ook in hoofdstuk 1 is verwoord, betekent dit niet dat daarbij als het ware onze achterdeur wagenwijd wordt openzet. Integendeel: voor de internationale uitwisseling van ongeëvalueerde gegevens is er één deur en die is voorzien van vier sloten. Allereerst kan enkel met anderen worden gedeeld wat rechtmatig door onze diensten is vergaard (eerste slot), waarbij geldt dat voor onderzoeksopdrachtgerichte interceptie toestemming van de minister is vereist en een positief rechtmatigheidsoordeel ter zake van de TIB. Ten tweede werken de Nederlandse diensten samen met betrouwbare partners, waarbij de uitwisseling van ongeëvalueerde gegevens slechts met een zeer beperkt aantal landen plaatsvindt. Eerbied voor de mensenrechten en democratische inbedding worden gewogen, voordat er wordt samengewerkt. Dat is nu ook opgenomen in het wetsvoorstel zelf (tweede slot). Het derde slot zorgt ervoor dat enkel gegevens kunnen worden uitgewisseld nadat de minister hier toestemming voor heeft gegeven. Tot slot, en dat is het vierde slot, houdt de CTIVD toezicht op deze praktijk. Dat heeft zij sinds 2002 ook meermaals gedaan en geconcludeerd dat het verstrekken van verzamelingen gegevens, zowel metagegevens als inhoudelijke communicatie, in de onderzochte samenwerkingsverbanden rechtmatig plaatsvindt.

In artikel 89, vierde lid, is de mogelijkheid tot het verlenen van technische en andere vormen van ondersteuning geregeld. Daarbij is hetzelfde afwegingskader aan de orde als

[149] Ongeëvalueerde gegevens kan zowel een enkel gegeven als een bulk aan gegevens omvatten.
[150] Ook waar het gaat om de verstrekking van ongeëvalueerde gegevens in het kader van de taakuitvoering van AIVD of MIVD.

bij de verstrekking van gegevens. Voor het verlenen van de hier bedoelde ondersteuning dient een door de bevoegde autoriteit van de desbetreffende buitenlandse collegadienst 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, Wiv 2002 is in artikel 89, zesde lid, van het wetsvoorstel 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*. Deze restrictie is niet meer opgenomen. Wel zijn er twee andere voorwaarden. De toestemming om ondersteuning te verlenen aan een buitenlandse dienst die als risicodienst wordt aangemerkt dient door de minister te worden gegeven.[151] Voorts zal, voor zover de ondersteuning betrekking heeft op de uitoefening van een bijzondere bevoegdheid als bedoeld in paragraaf 3.2.5, 4.2 of 4.3, de toestemming voor het geven van technische ondersteuning door de minister dienen te geschieden. In andere gevallen zou de bevoegdheid om in te stemmen met het verlenen van technische ondersteuning als zodanig, ook in niet spoedeisende gevallen, bij het hoofd van de dienst kunnen komen te liggen. Voor de goede orde zij opgemerkt dat indien het verzoek om ondersteuning tevens betekent dat de inzet van bijzondere bevoegdheden plaatsvindt door de dienst, er daarnaast voor de inzet van die bijzondere bevoegdheden toestemming dient te worden verleend. Voor die toestemming blijft het reguliere toestemmingsregime van de wet 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 collegadienst. Het ontbreken van het toestemmingsvereiste voor het doen van een verzoek aan een buitenlandse dienst om ondersteuning was reeds eerder door de CTIVD in de eerder gememoreerde rapporten nr. 22a (2009) en 22b (2015) 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. Inderdaad valt niet in te zien waarom een verzoek *van* een

[151] Onder risicodienst moet worden verstaan een dienst met wie de samenwerking op basis van de in artikel 88, derde lid, genoemde wegingscriteria een risico vormt.

buitenlandse dienst wel expliciet is geregeld in de wet maar een verzoek *aan* een buitenlandse dienst niet. De desbetreffende regeling is in artikel 90 van het wetsvoorstel neergelegd.

Artikel 90, 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 90 wordt onderscheid gemaakt tussen een aantal situaties. Allereerst de situatie waarin 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 die ingevolge het bij of krachtens deze wet bepaalde bevoegd is tot het verlenen van de toestemming voor de uitoefening van de desbetreffende bijzondere bevoegdheid (artikel 90, 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 er een waarin 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 3.2.5, 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 wanneer 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 verzoek om ondersteuning die niet in overeenstemming is met de aard en intensiteit van de samenwerkingsrelaties, zoals die naar aanleiding van de weging als bedoel in artikel 88 is vastgesteld, dient de toestemming altijd te worden verleend door de voor de dienst verantwoordelijke minister. Of door de desbetreffende buitenlandse collegadienst 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 doen van het verzoek; indien de buitenlandse collegadienst de verzochte ondersteuning verleent, moet deze geacht worden onder de verantwoordelijkheid van die dienst te worden uitgevoerd. In artikel 90, 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 90, 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 bevoegdheid als bedoeld in dit wetsvoorstel. Met deze regeling wordt aldus voorkomen dat men in de verzoeken om ondersteuning treedt buiten de bevoegdheden die ingevolge de wet (limitatief) aan de diensten toekomen. In het ter consultatie gezonden wetsvoorstel beperkte deze bepaling zich tot bijzondere bevoegdheden. Zoals ook in de PIA Wiv terecht is geconstateerd is er echter geen reden waarom deze bepaling zich tot bijzondere bevoegdheden zou moeten beperken en niet zou moeten zien op alle bevoegdheden als bedoeld in de wet.

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 91 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 91 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 KMar 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 91 wordt voorgesteld om ook de Hoofddirecteur van de 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 91, 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 91, 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 en de medewerkers van de Inspectie SZW bij de taakuitvoering van de AIVD zijn 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 91-functionarissen" aan te wijzen. Op dit moment worden de desbetreffende medewerkers door de AIVD overigens reeds als zodanig aangemerkt. Sinds december 2010 neemt ook de Inspectie SZW deel aan de CT-Infobox. Op grond van artikel 91, 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 91, 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 waarin deze ambtenaren overeenkomstig artikel 91 werkzaamheden voor de AIVD verrichten buiten toepassing te worden verklaard.

Artikel 92 van het wetsvoorstel voorziet in een met artikel 91 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 de Commissie Dessens[152] als de CTIVD[153] heeft de aanbeveling gedaan om de KMar ook werkzaamheden te kunnen laten verrichten op het militaire domein voor de MIVD. Er is gekozen om dit in een afzonderlijke bepaling te regelen en niet te incorporeren in het voorgestelde artikel 91. 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 91 (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 92, 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 91, 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 92, derde lid). Het betreft hier bijvoorbeeld werkzaamheden op luchthavens en grensovergangsplaatsen. In het vierde lid is ten slotte een met artikel 91, 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 92 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

[152] Rapport Commissie Dessens, *Evaluatie Wet op de inlichtingen- en veiligheidsdiensten 2002. Naar een nieuwe balans tussen bevoegdheden en waarborgen,* blz. 123.
[153] 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 87 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 93, 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, van de huidige wet reeds een informatieverplichting voor de hier bedoelde leden van het openbaar ministerie opgenomen. 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.[154] Teneinde elk misverstand daaromtrent te voorkomen, wordt voorgesteld dit nadrukkelijk in artikel 93, eerste lid, te stipuleren. In artikel 93, 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 94 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 94 in verschillende opzichten opnieuw geformuleerd. In artikel 94, 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 93 is ook met betrekking tot de in artikel 94 neergelegde informatieverplichting bepaald, dat de 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

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

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."[155] 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 93 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 94, 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.[156] Het huidige artikel 62 van de Wiv 2002 voorziet daar thans niet in. Artikel 94, 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 getroffen aan de kant van de desbetreffende dienst als maatregelen aan de kant van de instantie die de gegevens langs deze weg verstrekt.

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

In artikel 95 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 95, eerste tot en met derde lid, wordt voorgesteld.[157] 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. De verzochte ondersteuning wordt slechts verleend indien daarvoor toestemming is verkregen van de voor de ondersteunende dienst verantwoordelijke minister of namens deze het hoofd van de dienst. Indien de toestemming is verkregen voor 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. 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 voorzien dat in afwijking van het bepaalde in het tweede en derde lid in

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

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. Tevens is bepaald dat het verzoek in spoedeisende gevallen mondeling kan geschieden en dat deze vervolgens zo spoedig mogelijk schriftelijk wordt bevestigd. 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 die 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. Nader zal moeten worden bezien of het inderdaad nog nodig is voor de CT Infobox een regeling te treffen.

Artikel 96, 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. Externe controle op de inlichtingen- en veiligheidsdiensten vindt thans plaats door diverse instanties, maar vanuit verschillende invalshoeken. In paragraaf 7.2 wordt in het kort geschetst hoe het huidige stelsel is ingericht. Ten opzichte van het huidige stelsel worden in dit wetsvoorstel diverse aanpassingen voorgesteld, welke ertoe strekken om het toezicht in brede zin (vooraf, achteraf en in de sfeer van klachtbehandeling) te verstevigen. De regering is overtuigd dat hiermee – tezamen met diverse andere in dit wetsvoorstel voorziene waarborgen met name waar het gaat om de uitoefening van bijzondere bevoegdheden - op adequate wijze invulling wordt gegeven aan de eisen die uit artikel 8 en 13 EVRM voortvloeien. In hoofdstuk 9 van deze memorie van toelichting wordt daarop nader ingegaan.

In het wetsvoorstel zoals dat in internetconsultatie was gegeven, was op het vlak van toezicht en klachtbehandeling reeds voorzien in aanpassingen van het bestaande stelsel, met name op het vlak van toezicht en klachtbehandeling door de CTIVD en de rol van de Nationale ombudsman bij klachtbehandeling. Deze aanpassingen vloeiden voort uit de voorstellen van de Commissie Dessens, de reactie van de CTIVD daarop en de wijze waarop het kabinet heeft aangegeven daaraan uitwerking te willen geven. Uit de vele reacties naar aanleiding van de internetconsultatie is gebleken dat er door verschillende respondenten (naast vele burgers, ook door organisaties als het IVIR, NJCM, CRvdM en AI), maar ook door de CTIVD en de Nationale ombudsman, kanttekeningen worden geplaatst bij het EVRM-proof zijn van het eerder voorgestelde stelsel. Deels betrof het *systeemkritiek* – het stelsel als geheel zou niet voldoen aan het EVRM; en ook de scheiding tussen toezicht en klachtbehandeling zou niet voldoende zijn – en deels *kritiek op deelaspecten ervan* – met name de toestemmingverlening voor de meest ingrijpende bijzondere bevoegdheden (waarbij de focus zich in het bijzonder richtte op de nieuwe bevoegdheid tot bulkinterceptie van kabelgebonden telecommunicatie). In het bijzonder door het ontbreken van een vorm van onafhankelijke bindende toets – ex ante dan wel ex post (en volgens sommigen zelfs beide) - waar het gaat om de uitoefening van bijzondere bevoegdheden zou het voorgestelde stelsel (nog) niet voldoen aan de eisen van het EVRM; dus los van de mogelijkheid van bindende klachtbehandeling die met name vanuit het perspectief van artikel 13 EVRM van belang is. Een en ander is voor de regering aanleiding geweest om het stelsel als geheel nog eens kritisch te bezien. De observatie in de verschillende reacties dat de ontwikkeling – Europeesrechtelijk en internationaalrechtelijk – in de richting van een sterker onafhankelijk toezicht gaat wordt door ons gedeeld. Aangezien een van de doelen van het wetsvoorstel is om te voorzien

in een EVRM-proof stelsel, ook waar het gaat om toezicht, is ervoor gekozen om het in het concept-wetsvoorstel voorgestelde stelsel van toezicht- en klachtbehandeling aan te vullen met een onafhankelijke toets met betrekking tot de uitoefening van die bijzondere bevoegdheden waar de voor de dienst verantwoordelijke minister zelf toestemming voor dient te geven. Het betreft die bijzondere bevoegdheden die in het concept-wetsvoorstel waren onderworpen aan het zogeheten heroverwegingsstelsel.[158] Met de introductie van deze nieuwe onafhankelijke toets komt dat stelsel dan ook te vervallen. De onafhankelijke toets is opgedragen aan een nieuw in te stellen commissie, de Toetsingscommissie inzet bevoegdheden (TIB) (artikelen 32 tot en met 37 van het wetsvoorstel). Deze toets maakt onderdeel uit van het stelsel van toestemmingverlening met betrekking tot de desbetreffende bijzondere bevoegdheden en is dan ook opgenomen in het hoofdstuk inzake de verwerking van gegevens door de diensten, waarvan de bijzondere bevoegdheden deel uitmaken. Een door de minister verleende toestemming dient voordat deze kan worden geëffectueerd eerst door de TIB op rechtmatigheid te worden beoordeeld. Acht de TIB de toestemming rechtmatig, dan kan de desbetreffende bevoegdheid worden uitgeoefend; zo niet, dan vervalt de toestemming van rechtswege. In paragraaf 3.3.3 van de memorie van toelichting is op de voorgestelde regeling met betrekking tot de TIB nader ingegaan. In onderhavig hoofdstuk zal daar dan ook niet meer afzonderlijk aandacht aan worden geschonken. Op de implicaties van de introductie van een rechtmatigheidstoets door de TIB voor de toezichthoudende taak van de CTIVD is in paragraaf 3.3.3.1 van deze memorie van toelichting reeds ingegaan.

In paragraaf 7.3 zal ingegaan worden op de wijzigingen die anderszins worden voorgesteld ten opzichte van het in paragraaf 7.2 geschetste huidige stelsel.

De regering houdt aldus vast aan het toezichts- en klachtstelsel, zoals dat was opgenomen in het aan de Afdeling advisering van de Raad van State voorgelegde wetsvoorstel (en vult dat op het punt van de TIB conform het advies van de Afdeling

[158] In artikel 102 van het concept-wetsvoorstel,zoals dat in consultatie is gegeven, was ter zake de volgende regeling opgenomen:

1. Indien de afdeling toezicht in het kader de uitoefening van haar toezichthoudende taak tot de bevinding komt dat een door Onze betrokken Minister verleende toestemming als bedoeld in de artikelen 25, tweede lid, 27, derde lid, 28, tweede en vierde lid, 30, derde en zesde lid, 32, tweede lid, 33, tweede lid, 34, vierde lid, 35, tweede en vierde lid, 37, tweede lid, 38, tweede lid en 41, tweede lid, niet in overeenstemming is met hetgeen dat bij of krachtens deze wet is gesteld, kan zij Onze betrokken Minister daarvan op de hoogte stellen.
2. Onze betrokken Minister beziet zo spoedig mogelijk, doch uiterlijk binnen vijf werkdagen, naar aanleiding van een mededeling als bedoeld in het eerste lid, of de verleende toestemming in het licht van de bevindingen van de afdeling toezicht in stand kan worden gelaten.
3. Indien Onze betrokken Minister 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, doet hij daarvan terstond mededeling aan de afdeling toezicht alsmede aan de beide kamers der Staten-Generaal. Artikel 12, derde en vierde lid, is van overeenkomstige toepassing.

advisering aan), en wijst zij de conclusie van de Afdeling advisering dat het voorgestelde stelsel van toezicht als geheel niet toereikend zou zijn van de hand. De Afdeling advisering onderkent weliswaar dat met de introductie van voorafgaande toetsing door de TIB tegemoet wordt gekomen aan de voorkeur van het EHRM voor een bindende juridische toetsing vooraf, maar komt tot de conclusie dat hierdoor het stelsel van toezicht op de inzet van de diensten en de wijze waarop zij hun bevoegdheid uitoefenen in het geheel bezien onvoldoende effectief zal zijn. De Afdeling advisering is van oordeel dat de toetsing door de TIB in de praktijk zal neerkomen op een marginale en abstracte rechtmatigheidstoetsing ex ante. Daarbij komt, aldus de Afdeling advisering, dat het naast elkaar bestaan van de TIB en de CTIVD in verband met de daaruit voortvloeiende afstemmingsproblemen gemakkelijk afbreuk kan doen aan de effectiviteit van het toezicht. De Afdeling advisering acht het veeleer in de rede liggen om het toezicht bij de CTIVD te concentreren; in tegenstelling tot de TIB beschikt de CTIVD niet alleen over juridische kennis maar heeft zij ook inzicht in en overzicht van het daadwerkelijk handelen van de diensten. Zowel de toetsing ex ante als ex post zou bij de CTIVD moeten worden neergelegd met een verzwaarde heroverwegingsprocedure (vergelijk het concept-wetsvoorstel zoals in consultatie gegeven). Dit zou wel met zich meebrengen dat de klachtbehandeling niet door de CTIVD zou moeten plaatsvinden; toezicht en klachtbehandeling zouden strikt gescheiden moeten zijn, opdat zelfs de schijn van partijdigheid wordt vermeden. Gelet daarop adviseert de Afdeling advisering om de klachtregeling zoals thans in de Wiv 2002 is neergelegd ongewijzigd te laten.

De regering deelt de door de Afdeling advisering getrokken conclusie niet vanwege de volgende redenen. De regering heeft bij de voorbereiding van het wetsvoorstel zelf een uitvoerige analyse gemaakt van de jurisprudentie van het EHRM met betrekking tot met name artikel 8 en 13 EVRM en de gevolgen die daaraan zouden moeten worden verbonden voor de inrichting van onderhavig wetsvoorstel; zowel voor de te treffen waarborgen bij de aan de diensten toe te kennen bevoegdheden, maar ook waar het gaat om het stelsel van toezicht (in brede zin) en klachtbehandeling. In hoofdstuk 9 van de memorie van toelichting wordt daarop uitgebreid ingegaan. Deze analyse, die naar ons oordeel op zijn minst op hoofdlijnen wordt gedeeld door diverse instanties die gespecialiseerd zijn in mensenrechtelijke vraagstukken en die in de internetconsultatie hebben gereageerd en in de gevolgen die daaraan verbonden moeten worden op onderdelen zelfs verder gaan dan de regering voorstelt (zoals niet alleen bindende toets ex ante, maar ook ex post)[159], wijst – in ieder geval in de gevolgen die daaraan verbonden zouden moeten worden - in een geheel andere richting dan de Afdeling advisering suggereert. Daaraan voegen we toe dat de normen van het EVRM (en de

[159] Zie het overzicht in hoofdstuk 12 van de memorie van toelichting.

uitwerking daarvan in de jurisprudentie van het EHRM) zijn aan te merken als minimum-normen; niets verzet zich ertegen dat een verdragsstaat in zijn eigen wetgeving hogere normen hanteert. De opmerking van de Afdeling advisering dat bij de beantwoording van de vraag of in een verdragsstaat bij het EVRM sprake is van een daadwerkelijk rechtsmiddel (artikel 13 EVRM) *het geheel* van beschikbare voorzieningen door het EHRM wordt beoordeeld onderschrijven wij; echter artikel 8 EVRM – waarop de Afdeling advisering niet of nauwelijks als zodanig ingaat – eist dat bij diep in de persoonlijke levenssfeer ingrijpende bevoegdheden wordt voorzien in "effective guarantees against abuse". Een onafhankelijke bindende toets voorafgaand aan de inzet van een bevoegdheid door een rechter (of een andere daarmee vergelijkbare instantie) heeft daarbij de voorkeur. Het is met name in dit licht dat de introductie van de TIB moet worden bezien; de regering is van oordeel dat het achterwege laten van een voorziening als de TIB het risico te groot is dat aldus niet wordt voldaan aan de eisen van het EVRM en bij een toets door het EHRM als te licht wordt bevonden met alle gevolgen vandien. Dat risico wil de regering niet lopen, zeker nu met het wetsvoorstel wordt gestreefd naar een toekomstvaste regeling voor de activiteiten van de inlichtingen- en veiligheidsdiensten. Het door de Afdeling advisering gepresenteerde alternatief van een ex ante en ex post toets zonder een bindend element (maar met een verplichte heroverweging door de minister) voldoet naar ons oordeel niet; het feit dat de ministers over het algemeen het oordeel van de CTIVD onderschrijven, doet daar niet aan af. Daar komt bij dat bij het beleggen van een ex ante en een ex post toets bij de CTIVD dezelfde bezwaren kunnen voordoen als de Afdeling advisering schetst bij het positioneren van toezicht en klachtbehandeling bij de CTIVD; in het toezicht achteraf door de CTIVD zou men immers ook toezicht houden op de eerdere ex ante verrichte toetsing op concept-besluiten tot inzet van bijzondere bevoegdheden. Mede gelet daarop is juist in het wetsvoorstel voorzien in een strikte scheiding tussen de uitoefening van het rechtmatigheidstoezicht en de behandeling van klachten bij de CTIVD door de instelling van twee afzonderlijke afdelingen waarvan de leden niet in beide afdelingen tegelijk kunnen zitten. Deze scheiding dient naar het oordeel van de regering ook door te werken tot op het niveau van de ambtelijke ondersteuning.[160] Met de Afdeling advisering is de regering het overigens eens dat toezicht niet alleen formeel aan de eisen van het EVRM dient te voldoen, maar ook in materieel opzicht effectief dient te zijn. Zoals eerder aangegeven, zijn de adviezen van de Afdeling advisering tot versterking van de TIB onverkort overgenomen; verder is het slechts een kwestie van tijd – benodigd voor opbouw van kennis en expertise inzake de werkzaamheden van de diensten – voordat de TIB voor de taak waarvoor zij zich wettelijk gesteld ziet, als voldoende effectief (in

[160] Zie ook de Wet Huis voor klokkenluiders die een vergelijkbare voorziening heeft voor zowel de leden van de twee afdelingen (zie artikel 3b) als de medewerkers van het bureau (artikel 3d).

materiële zin) kan worden aangemerkt. Ook de CTIVD is immers in een kort tijdsbestek tot een gezaghebbend en deskundig geacht instituut uitgegroeid. De regering ziet niet in waarom de TIB niet een vergelijkbare ontwikkeling zou kunnen doormaken.

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.[161] De voorzitters van tussentijds ontstane fracties zijn niet in de CIVD vertegenwoordigd.

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.[162] 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)

[161] Zie artikel 22, tweede lid, jo. artikel 11, eerste lid, Reglement van Orde voor de Tweede Kamer der Staten-Generaal.
[162] 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.

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.[163] 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 de regering 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.

De Commissie voor de Inlichtingen- en Veiligheidsdiensten (CIVD) heeft bij brief aan de Vaste Kamercommissie voor Binnenlandse Zaken d.d. 10 december 2015 bericht over de uitkomsten van haar onderzoek naar een versterking van haar functioneren. In deze brief is de taak van de CIVD om de operationele taakuitvoering van de AIVD en de MIVD te controleren opnieuw benadrukt. Tevens zijn de uitgangspunten geformuleerd dat het kabinet de informatie over de AIVD en de MIVD zoveel mogelijk als openbare stukken aan de Kamer aanbiedt en dat de CIVD in beginsel geen vertrouwelijke stukken in behandeling neemt die betrekking hebben op andere onderwerpen dan op de uitvoering

[163] Zie artikel 8, vierde lid, Wiv 2002.

van de operationele taak van de AIVD en de MIVD. Met betrekking tot de samenstelling en ondersteuning van de CIVD is besloten om de huidige samenstelling van de CIVD, met de fractievoorzitters als leden, te handhaven.

De CIVD heeft een aantal verbeterpunten geformuleerd:

- De introductie voor nieuwe CIVD-leden wordt verder geprofessionaliseerd door het samenstellen van een introductiepakket.
- Aan het Presidium van de Tweede Kamer zal een wens tot uitbreiding van de ambtelijke staf worden voorgelegd.
- De wisselwerking tussen de CIVD enerzijds en de CTIVD en de Algemene Rekenkamer anderzijds zal worden versterkt.
- Met betrekking tot de informatievoorziening zal in het vervolg worden gewerkt met een verder gestructureerde inhoudelijke jaarplanning.

Ook is in het onderzoek expliciet aandacht besteed aan de spanning tussen de noodzakelijke geheimhouding en de wens om zoveel als mogelijk parlementaire controle in de openbaarheid te laten plaatsvinden. De CIVD heeft met de betrokken ministers afgesproken dat deze zich zullen inspannen voor een zo duidelijk en zo fijnmazig mogelijk onderscheid tussen openbare en geheime informatie, en een duidelijke onderbouwing waarom bepaalde informatie geheim is. Ten aanzien van de mate waarin de CIVD meer openheid wil bieden over de onderwerpen waarover zij is geïnformeerd en wat dit betekent voor de manier waarop de fractievoorzitters daarmee binnen hun fractie omgaan, is besloten dat het in principe achteraf niet geheim is dat er is vergaderd en op welke dag. De overige informatie over vergaderingen en agenda's blijft onder de geheimhouding vallen. Jaarlijks zal de CIVD – zoals nu al gebruikelijk is – in het openbaar verslag uitbrengen van haar werkzaamheden.

Uiteraard is het aan de Tweede Kamer zelf om te bepalen op welke wijze men de parlementaire controle wenst in te richten. De regering stelt enkel als voorwaarde dat waar geheimhouding wordt betracht, deze ook absoluut kan worden gegarandeerd en dat het stelsel eenduidig is. De uitkomsten van het onderzoek van de CIVD zijn niet strijdig met deze voorwaarden.

Toezicht door de Commissie van Toezicht op 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 de regering, dat bij de keuze voor de persoon die de vacature gaat vervullen aan die voordracht is gebonden. Indien de regering geen van de voorgedragen kandidaten geschikt acht, vraagt de regering 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.[164]

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;

- 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 Awb van toepassing, zij het dat er op een enkel punt is voorzien in een afwijking (artikel 83, derde en vierde lid, Wiv 2002) 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

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

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 Wvo (zoals de weigering of intrekking van een verklaring van geen bezwaar) worden voorgelegd aan de bestuursrechter. Het bestuursprocesrecht van de Awb 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 klachtstelsel

7.3.1 Algemeen

Ten opzichte van het in paragraaf 7.2 geschetste stelsel, wordt in het wetsvoorstel – naast de invoering van een onafhankelijke toets door de TIB – voorzien in een aantal aanpassingen die niet alleen leiden tot versterking van het klachtstelsel maar ook de mogelijkheid bieden om voortaan vermoedens omtrent misstanden bij de CTIVD te melden (“klokkenluidersregeling”). Deze aanpassingen brengen belangrijke wijzigingen met zich mee in de bestaande regeling voor toezicht- en klachtbehandeling die aan de CTIVD is opgedragen. 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, 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).

Thans zal worden ingegaan op de verschillende wijzigingen.

7.3.2 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.[165] 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. Ook de Afdeling advisering van de Raad van State wijst in haar advies op deze problematiek. Voorts stelt de Commissie Dessens dat dit argument wordt versterkt als het voorstel van de commissie wordt gevolgd, waarbij het rechtmatigheidsoordeel van

[165] Rapport van de Commissie Dessens, *Evaluatie Wet op de inlichtingen- en veiligheidsdiensten 2002. Naar een nieuwe balans tussen bevoegdheden en waarborgen*, p. 151 e.v.

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 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 97, 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 en de Wvo 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 113 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 97, 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 97, 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 98, 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 99, 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 102).

De CTIVD alsmede haar afdelingen worden ondersteund door een secretariaat; artikel 103 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. Het is aan de CTIVD gelaten om daarvoor intern een regeling te treffen.

7.3.3 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 Awb 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.

7.3.4 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 – zoals dat wel het geval is met betrekking tot titel 9.1 Awb - onverkort van toepassing kan zijn (artikel 114, eerste lid, laatste volzin). 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.

7.3.5 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 114 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 114 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.[166] Het moet dan niettemin mogelijk zijn om een klacht in te dienen.

De artikelen 115, 116 en 117 hebben betrekking op de ontvankelijkheid van een klaagschrift, de onpartijdigheid van de klachtbehandelaar en op de mogelijkheid voor de 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 118 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 119 bevat, net als artikel 9:19 van de Awb, regels ter zake van een mogelijke samenloop met bezwaar, beroep of beklag.

De artikelen 120 tot en met 123 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

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

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 124 van het wetsvoorstel heeft betrekking op het oordeel van de afdeling klachtbehandeling. De afdeling klachtbehandeling beoordeelt of in de door haar onderzochte aangelegenheid behoorlijk is gehandeld. Een toets aan behoorlijkheid omvat ook een toets aan rechtmatigheid als één van de behoorlijkheidnormen. 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 de onafhankelijke toets door de TIB in de toestemmingsfase (ex ante) en het rechtmatigheidstoezicht door de afdeling toezicht van de CTIVD(ex post) - 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 124, 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. Het ligt derhalve in de rede dat de afdeling klachtbehandeling in geval van twijfel in dit kader de betrokken minister raadpleegt. 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 niet 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 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 124, 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.

7.3.6 Gevolgen voor de Nationale ombudsman

Artikel 114, eerste lid, laatste volzin, 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. De Nationale ombudsman heeft in zijn reactie op het concept-wetsvoorstel aangegeven dat met het voorstel wordt afgeweken van de bestaande wettelijke structuur, waarin voor de Nationale ombudsman als sluitstuk in de sfeer van de behandeling van klachten over inlichtingen- en veiligheidsdiensten een rol is weggelegd. De Nationale ombudsman vindt het onverantwoord om de klachtbehandeling te positioneren in een aparte kamer klachtbehandeling bij de CTIVD. De Nationale ombudsman wijst erop dat risico bestaat dat de klachtbehandeling niet onafhankelijk en onpartijdig is, terwijl de verruimde bevoegdheden te meer onafhankelijke rechtsbescherming vereisen. Hij pleit er dan ook voor om de klachtbehandeling onder te brengen bij een evident onafhankelijk en onpartijdig instituut, zoals de Nationale ombudsman.

Voor een (rest)taak voor de Nationale ombudsman ziet de regering geen aanleiding, nu de bevoegdheden van de afdeling klachtbehandeling van de CTIVD, zowel met betrekking tot de te volgen procedure als met betrekking tot het bindendheid van het oordeel, zoals hiervoor is toegelicht, aanzienlijk verder strekken dan die welke de Nationale ombudsman toekomen.

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 125quinquies, 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 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."[167]

Daarom zijn in de Wet Huis voor klokkenluiders 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 uitgezonderd van het kunnen doen van een melding van een vermoeden van een misstand bij het Huis van de klokkenluiders (artikel 4, tweede lid).

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 125, onderdeel a, ruim gedefinieerd. Het is een ieder die betrokken is of is geweest bij de Wet op de inlichtingen en veiligheidsdiensten–

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

of bij de Wvo en die een melding doet. Voor deze ruime formulering is 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.[168] 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 128, eerste lid, aanhef en 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 125, onderdeel c). Uitgangspunt is bovendien dat de melder de melding eerst doet bij de organisatie waar de vermoede misstand zich afspeelt (artikel 126, 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 126, tweede lid). In artikel 126, derde en vierde lid, is nader aangegeven wat de melding ten minste aan gegevens dient te

[168] De uitzondering in artikel 4, tweede lid, onder b, van de Wet Huis voor klokkenluiders wordt bij inwerkingtreding van onderhavig wetsvoorstel daarmee in lijn gebracht; zie daartoe artikel 156 van het wetsvoorstel.

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 127, 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 127, tweede lid). In artikel 128 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 129).

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 131). 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 130).

In artikel 131, 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 131, 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 23 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 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 135 en 136 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 personen te doen uitstrekken. Gewezen wordt onder meer op artikel 66, vierde lid, en 68, 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 135 richt zich tot een ieder die betrokken is bij de uitvoering van de wet en artikel 136 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 137 ziet daarbij op bestuursrechtelijke procedures en artikel 138 op civielrechtelijke procedures. Ter toelichting wordt het volgende opgemerkt.

Artikel 137

Het huidige artikel 87, eerste lid, van de Wiv 2002 bepaalt dat in bestuursrechtelijke procedures inzake de toepassing van de Wiv 2002 of de Wvo 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 CTIVD door de rechtbank ingevolge de artikelen 8:27, 8:28 of 8:45 van de 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 2002 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.[169] Het kabinet heeft deze aanbeveling overgenomen.[170]

In het nieuwe artikel 137 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 voornoemde 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 137 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

[169] Zie het rapport van de Commissie Dessens, *Evaluatie Wet op de inlichtingen- en veiligheidsdiensten 2002. Naar een nieuwe balans tussen bevoegdheden en waarborgen*, par. 7.5 (blz. 152 e.v.).
[170] Zie de kabinetsreactie op het rapport van de Commissie Dessens van 11 maart 2014 (kamerstukken II 2013/14, 33 820, nr. 2).

oordeel van de rechter, dat het onthouden van geheime stukken aan een procespartij 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 137, 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 137 is een soortgelijke regeling als bedoeld in het eerste 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 137, eerste en tweede lid, is naar zijn werking beperkt tot bestuursrechtelijke procedures inzake de toepassing van de Wiv en de Wvo; procedures waarbij derhalve de betrokken minister partij is. De problematiek waarvoor artikel 137 een oplossing geeft, is er echter niet alleen een die zich voordoet in de gevallen waartoe het huidige artikel 87 Wiv 2002 zich nu beperkt. Ook in de gevallen dat er geen sprake is van een bestuursrechtelijke procedure inzake de toepassing van de Wiv 2002 en de Wvo 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 137 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 62, eerste lid, onder a en b.

Artikel 137, vierde lid, 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 138

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.[171] Het nieuwe artikel 138 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 daarin volhardt, brengen volgens de Hoge Raad de eisen van een behoorlijke

[171] Zie het rapport van de Commissie Dessens, *Evaluatie Wet op de inlichtingen- en veiligheidsdiensten 2002. Naar een nieuwe balans tussen bevoegdheden en waarborgen*, par. 7.5 (blz. 152 e.v.).

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 138. Vanwege de beknoptheid van artikel 22 van het Wetboek van Burgerlijke Rechtsvordering is de civielrechtelijke procedure in artikel 138 wat meer uitgewerkt dan de bestuursrechtelijke procedure in artikel 137. 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 139

Artikel 139 is ongewijzigd gebleven ten opzichte van het huidige artikel 88 Wiv 2002. 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 Inleiding

De taken van de inlichtingen- en veiligheidsdiensten kunnen vanwege hun aard inbreuk maken op het privéleven van de personen waarnaar de diensten 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 binnendringen van een geautomatiseerd werk, 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.[172] Het verzamelen en verwerken van gegevens over het privéleven van burgers in het belang van de nationale veiligheid vormen een inbreuk van het recht op eerbiediging van de persoonlijke levenssfeer[173] 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). De toetsing van onderhavig wetsvoorstel aan bescherming van de persoonlijke levenssfeer en aanverwante rechten vindt plaats in de paragrafen 9.2 tot en met 9.4.

Ook andere grondrechten kunnen bij de inzet en uitvoering van de bevoegdheden van de inlichtingen- en veiligheidsdiensten in beeld komen; zo heeft eenieder volgens artikel 13 EVRM recht op een daadwerkelijk en effectief rechtsmiddel. 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. De implicaties van het wetsvoorstel op dit grondrecht worden uitgewerkt in paragraaf 9.5.

Tot slot dient aandacht te worden besteed aan het recht op een eerlijk proces; informatie van de AIVD en de MIVD kan immers 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. Hierop wordt nader ingegaan in paragraaf 9.6.

Het handelen van de inlichtingen en veiligheidsdiensten valt op grond van artikel 4, tweede lid, van het Verdrag van de Europese Unie buiten de bevoegdheden van de Europese Unie. De verwerking en bewaring van persoonsgegevens valt door inlichtingendiensten gelet op deze bepaling eveneens buiten de reikwijdte van de EU privacy instrumenten. Het Handvest voor de Grondrechten van de EU is van toepassing alleen voor zover de lidstaten uitvoering geven aan Unierecht. Wanneer met de activiteiten van de inlichtingen- en veiligheidsdiensten uitvoering wordt gegeven aan het EU recht komen zij binnen de werkingssfeer van het Handvest.

9.2 Het recht op bescherming van de persoonlijke levenssfeer

[172] *Democratic and effective oversight of national security services*, Council of Europe Commissioner for Human Rights, Straatsburg, mei 2015.
[173] Met het recht op het privéleven of het recht op privacy wordt in dit wetsvoorstel hetzelfde bedoeld.

De persoonlijke levenssfeer is een niet nader afgebakend begrip waaronder uiteenlopende aspecten van het persoonlijke leven worden geschaard. Een aantal in relatie tot de inlichtingen- en veiligheidsdiensten relevante aspecten van het recht op bescherming van de persoonlijke levenssfeer zijn in artikel 8, eerste lid van het EVRM, en in artikel 10 tot en met 13 van de Grondwet nader uitgewerkt in aparte rechten. Zij worden ook geduid als de vier dimensies van de persoonlijke levenssfeer, te weten de informationele, lichamelijke, ruimtelijke en relationele privacy. Artikel 8, eerste lid, van het EVRM belichaamt expliciet een aantal dimensies van de persoonlijke levenssfeer, te weten het algemene begrip persoonlijke levenssfeer, de ruimtelijke (woning) en de relationele (correspondentie en familie- en gezinsleven) privacy. De informationele en de fysieke dimensie van de persoonlijke levenssfeer zijn in de rechtspraak van het EHRM tot ontwikkeling gekomen. Het toetsingskader dat volgt uit het EVRM en de jurisprudentie van het EHRM is derhalve op de verwerking van persoonsgegevens van toepassing. In de Grondwet zijn de vier dimensies van de van de persoonlijke levenssfeer, te weten de informationele, lichamelijke, ruimtelijke en relationele privacy achtereenvolgens te vinden in het recht op gegevensbescherming (artikel 10, tweede en derde lid, van de Grondwet), het recht op lichamelijke integriteit (artikel 11 Grondwet), het recht op bescherming van het huisrecht (artikel 12 Grondwet) en het recht op bescherming van de communicatie die via een middel verloopt (artikel 13 Grondwet). Getoetst wordt of het wetsvoorstel de toets van de hiervoor genoemde grondwettelijke en verdragsrechtelijke vereisten doorstaat.

9.2.1 Toetskader artikel 8 EVRM

Elke beperking van het recht op bescherming van de persoonlijke levenssfeer ten behoeve van de nationale veiligheid dient te voldoen aan artikel 8 EVRM.[174] Het EVRM stelt in artikel 8 gelet op verwijzing naar legaliteit en noodzakelijkheid en anders dan de Grondwet materiële eisen waaraan een inbreuk op de persoonlijke levenssfeer dient te voldoen. Het wetsvoorstel voorziet in een stelsel van adequate waarborgen dat aan deze eisen tegemoet komt. Limitatief is daarin vastgelegd onder welke voorwaarden 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 garanderen dat een inbreuk op de persoonlijke levenssfeer die de inzet van bijzondere bevoegdheden in het belang van de nationale veiligheid tot gevolg kan hebben, toch in balans is met het

[174] Artikel 8 EVRM luidt: '1. Een ieder heeft recht op respect voor zijn privéleven, zijn familie- en gezinsleven, zijn woning en zijn correspondentie. 2. Geen inmenging van enig openbaar gezag is toegestaan in de uitoefening van dit recht, dan voor zover bij de wet is voorzien en in een democratische samenleving noodzakelijk is in het belang van de nationale veiligheid […]'

recht op bescherming van de persoonlijke levenssfeer van de burger. De jurisprudentie van het EHRM biedt een interpretatief kader van hetgeen onder deze eisen dient te worden verstaan, en wanneer inbreuken gerechtvaardigd kunnen worden.

Het toetskader aan de hand waarvan dat wordt bepaald, is vervat in de eisen van legaliteit (voorzienbaarheid bij wet) en noodzakelijkheid uit artikel 8, tweede lid, van het EVRM. Onder voorzienbaarheid valt niet alleen de vraag of de inbreuk is geregeld in een formele wet (of nadere vorm van regelgeving die voldoende inzichtelijk is voor burgers), maar ook de vraag of de wet voldoende kwaliteit heeft: is de inbreuk voldoende gedetailleerd uitgewerkt en met voldoende precieze, effectieve waarborgen omkleed?[175] Onder noodzakelijkheid in een democratische samenleving wordt verstaan of zij voldoen aan de vereisten van proportionaliteit (de keuze voor het middel dat in verhouding staat tot het te realiseren doel) en subsidiariteit (de keuze voor minst ingrijpende middel dat geschikt is om het doel te bereiken), waarbij een beoordeling dient plaats te vinden of de voorgenomen maatregelen kunnen worden gerechtvaardigd door een 'pressing social need'.[176]

EVRM-eisen ten aanzien van legaliteit: kenbaarheid en voorzienbaarheid van inbreukmakende maatregelen

Een inbreuk op artikel 8 EVRM vergt gelet op het kenbaarheidsvereiste uit de EHRM-jurisprudentie een deugdelijke wettelijke basis.[177] Met betrekking tot de voorzienbaarheid van de wetgeving volgt uit de jurisprudentie van het EHRM[178] dat dit vereiste, gelet op de context waarin de inlichtingen- en veiligheidsdiensten opereren, niet zo ver gaat dat een persoon steeds in staat moet zijn precies te voorzien wanneer een inlichtingen- of veiligheidsdienst zijn communicatie zou willen onderscheppen, zodat hij zijn gedrag daarop kan aanpassen. Wel moet een persoon in staat worden gesteld om in redelijkheid te voorzien dat onder omstandigheden zijn gedrag kan leiden tot actie van de zijde van de diensten.[179] Om het risico van willekeur en misbruik tegen te gaan, dient de wet wel voldoende helder te zijn over de gevallen en de voorwaarden waaronder de autoriteiten de bevoegdheid hebben om inbreuk te maken op het recht op de

[175] 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. Zie ook *Kruslin t. Frankrijk*, par. 33 en 35 en EHRM 24 april 1990, *Huvig t. Frankrijk*, par. 32 e.v..
[176] Artikel 17 van het IVBPR volgt voor wet betreft voorwaarden waaronder het daarin neergelegde recht op eerbiediging van het privéleven 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, zie Human Rights Committee, General Comment nr 16.
[177] Onder meer EHRM 16 februari 2000, *Amman t. Zwitserland* en EHRM 4 mei 2000, par. 65 en *Rotaru t. Roemenie*, par. 43.
[178] EHRM augustus 1984, *Malone t. Verenigd Koninkrijk*, par. 67, EHRM 26 maart 1987, *Leander t. Zweden*, par. 51.
[179] EHRM 26 april 1979, *Sunday Times t. Verenigd Koninkrijk* 1979, serie A nr. 30, par. 49.

persoonlijke levenssfeer en dient het toezicht daarop voldoende stevig te zijn.[180] Dat betekent dat de wetgeving gedetailleerde regels moet geven voor het inzetten van bevoegdheden, zoals bijvoorbeeld ten aanzien van de interceptie van communicatie. 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.[181]

EVRM-eisen aan de waarborgen in de toezichtsystematiek

Het EHRM heeft in zijn jurisprudentie meermaals benadrukt onafhankelijk toezicht voorafgaand aan en tijdens de inzet van de bijzondere bevoegdheden te eisen. Het EHRM beoordeelt het nationale toezichtsysteem rondom inlichtingen- en veiligheidsdiensten in zijn geheel, dat wil zeggen voorafgaand aan de inzet van de inbreukmakende bevoegdheden, gedurende de uitvoering van de bevoegdheid en in de fase nadat de maatregelen beëindigd zijn. Het EHRM heeft in zijn jurisprudentie meermaals een voorkeur uitgesproken voor een rechterlijke toets voorafgaand aan de inzet van bevoegdheden, al heeft het in concrete gevallen ook een systeem van toezicht achteraf door een effectieve, onafhankelijke instantie in overeenstemming met het EVRM bevonden.[182] Hieronder zal nader worden ingegaan op welke wijze het toezichtsysteem in het wetsvoorstel tegemoet komt aan de vereisten van het EVRM.

EVRM-eisen ten aanzien van de gegevensverwerking

In 2006 heeft het EHRM in het arrest *Weber en Saravia tegen Duitsland* zijn jurisprudentie met betrekking de minimumwaarborgen rondom tot het gericht aftappen van telecommunicatie (in *Weber* betrof het telefoontaps) nader uitgewerkt. De volgende minimum waarborgen dienen in wetgeving te zijn uitgewerkt teneinde misbruik van (de interceptie)bevoegdheid te voorkomen.[183] In de (formele) 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 interceptiebevoegdheid; 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.

[180] Zie voor dit vereiste onder meer EHRM 4 mei 2000, *Rotaru t. Roemenië*, par. 59 en
[181] EHRM 25 maart 1983, *Silver en anderen t. Verenigd Koninkrijk*, par. 88 en EHRM 26 maart 1987, *Leander t. Zweden*, par. 51.
[182] EHRM 6 september 1978, *Klass en anderen t. Duitsland*, par. 55- 56,EHRM 18 mei 2010, *Kennedy t. Verenigd Koninkrijk*, par. 167 en 184-191 en EHRM 12 januari 2016, *Szabo en Vissy t. Hongarije*, par. 79.
[183] EHRM 29 juni 2006, *Weber en Saravia t. Duitsland*, par. 95, EHRM 1 juli 2008, *Liberty en anderen t. Verenigd Koninkrijk*, par. 62, 63 en *Roman Zakharov t. Rusland*, EHRM 4 december 2015, par. 229.

Deze voorwaarden heeft het EHRM in *Weber en Saravia ten Duitsland* toegespitst op de gerichte interceptie van telecommunicatie, maar de voorwaarden zijn in brede zin ook 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.[184] Overigens heeft het EHRM in *Uzun tegen Duitsland*[185], waarbij het ging om het via een GPS-systeem volgen van de bewegingen van een persoon in de openbare ruimte, deze strikte standaarden niet toegepast; het volgen van bewegingen via een GPS-systeem achtte het EHRM een minder vergaande inbreuk op de privacy van de betrokkene dan het afluisteren van diens telefoon, waardoor in dat concrete geval met minder zware waarborgen kon worden volstaan.

Waarborgen in het wetsvoorstel ten behoeve van legaliteit: kenbaarheid en voorzienbaarheid

De maatregelen in het wetsvoorstel dienen vanwege het heimelijk karakter ervan en vanwege de mogelijkheden die de technologie biedt omkleed te zijn met effectieve waarborgen teneinde tegenwicht te kunnen bieden aan het risico op misbruik. Ter borging daarvan zijn regels omtrent onafhankelijk toezicht en een onafhankelijke klachtenprocedure in het wetvoorstel opgenomen. Gelet op het gegeven dat de inlichtingen- en veiligheidsdiensten persoonsgegevens verwerken, zijn eveneens waarborgen rondom de gegevensverwerking opgenomen, zoals bewaartermijnen en voorwaarden waaronder persoonsgegevens kunnen worden gedeeld. In het onderhavige wetsvoorstel worden ten aanzien van de bijzondere bevoegdheden van de inlichtingen- en veiligheidsdiensten de zware eisen als uitgangspunt gehanteerd. In het wetsvoorstel is uitvoering gegeven aan zowel de vereisten die volgen uit de jurisprudentie van het EHRM, als aan het vereiste dat de bevoegdheden in voldoende detail worden beschreven. Hieronder wordt aan de hand van diverse aspecten met betrekking tot de vereiste legaliteit nader toegelicht op welke wijze daarin in het wetsvoorstel tegemoet wordt gekomen.

Kenbaarheid

Teneinde gevolg te geven aan het vereiste van het EVRM dat bevoegdheden voldoende kenbaar zijn is in navolging van adviezen van de CTIVD een aantal bevoegdheden van een expliciete wettelijke basis voorzien. De regering streeft in navolging van deze adviezen uitdrukkelijk naar een kenbare en voorzienbare beschrijving van de

[184] EHRM 1 juli 2008, *Liberty en anderen t. Verenigd Koninkrijk*, par. 63 en EHRM 12 januari 2016, *Szabó en Vissy t. Hongarije*, par. 55 en 66 e.v..
[185] EHRM 2 september 2010, *Uzun t. Duitsland*, par. 66. Het EHRM herbevestigde de vereisten uit *Weber en Saravia t. Duitsland* in EHRM 4 december 2008, *S. en Marper t. Verenigd Koninkrijk*, par. 99.

bevoegdheden. 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 43 van het wetsvoorstel) en de mogelijkheid om aan een verzoek om gegevens te voldoen door het verlenen van rechtstreekse geautomatiseerde toegang. In andere bepalingen is aangesloten bij de voortgeschreden technische en elektronische ontwikkelingen, zoals in artikel 48 van het wetsvoorstel, dat naast de interceptie van niet-kabelgebonden communicatie nu ook de interceptie van kabelgebonden communicatie regelt. Dit heeft tot gevolg dat de kenbaarheid van de wetgeving verder wordt vergroot.

Voorzienbaarheid: toebedeling van de bevoegdheden

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 in beide artikelen is gegeven volgt dat beide diensten zich richten op dreigingen tegen de nationale veiligheid. Dit uitgangspunt is leidend ten aanzien van het karakter van de gedragingen die tot de inzet van een bijzondere bevoegdheid kunnen leiden. 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. Zo kan door het parlement worden gecontroleerd of de diensten zich ook aan hun opdracht houden.

De *bijzondere* bevoegdheden van de diensten om gegevens te verzamelen en te verwerken mogen ingevolge artikel 28, eerste lid, 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 (mogelijk graverende) inbreuk die de bijzondere bevoegdheden kunnen maken op de persoonlijke levenssfeer van burgers.[186] Voor de overige taken van de inlichtingen- en veiligheidsdiensten (het verrichten van veiligheidsonderzoeken, de beveiligingsbevorderende taak en het opstellen van dreigings- en risicoanalyses) dienen de diensten zich te beperken tot de andere in artikel 25, eerste lid, van het wetsvoorstel genoemde bevoegdheden tot het verzamelen van gegevens. De beperking van de inzet van bijzondere bevoegdheden tot de uitvoering van

[186] 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.

een limitatief aantal taken van de diensten was al geregeld in de Wiv 2002. Hierin beoogt het wetsvoorstel in essentie geen verandering te brengen.

Voorzienbaarheid: eisen aan de verwerking van gegevens

In hoofdstuk 3 van het wetsvoorstel worden nauwkeurige regels gegeven voor de verzameling en verwerking 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 3.2 van het wetsvoorstel worden de diverse bevoegdheden tot het verwerken van gegevens geregeld; het betreft een limitatieve opsomming. Per bevoegdheid staat beschreven wat de omvang van de betreffende bevoegdheid is en welke procedures bij de uitoefening in acht moeten worden genomen ten aanzien van de duur van de toestemming, de bewaartermijn van de verworven gegevens en voor welke doeleinden en door wie de gegevens geanalyseerd mogen worden. Als uitgangspunt geldt dat de waarborgen zwaarder worden naarmate het inbreukmakende karakter van een bijzondere bevoegdheid groter wordt.[187]

In artikel 19 van het wetsvoorstel wordt onder meer de kring van personen weergegeven over wie gegevens mogen worden verwerkt. Deze bepaling stelt aanvullende eisen die worden gesteld aan de verwerking van bepaalde 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). Naast het bepaalde in artikel 19, derde lid, betreft het bijvoorbeeld ook het bewaren en vernietigen van celmateriaal en van de DNA-profielen (artikel 43) die op basis daarvan zijn opgesteld. Op de bevoegdheid tot het verrichten van DNA-onderzoek wordt hieronder afzonderlijk ingegaan.

In artikel 27 van het wetsvoorstel zijn nieuwe bepalingen opgenomen die vereisen dat gegevens die met bijzondere bevoegdheden zijn verzameld zo spoedig mogelijk worden onderzocht op hun relevantie voor het onderzoek waarvoor ze zijn verworven. Gegevens waarvan is vastgesteld dat deze niet relevant zijn voor het onderzoek dan wel enig ander lopend onderzoek vallend onder de taken, bedoeld in artikel 8, tweede lid, onder a en d, en artikel 10, tweede lid, onder a, c en e, worden na een termijn van maximaal twaalf maanden vernietigd (deze termijn kan eenmalig met zes maanden worden verlengd). 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

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

van maximaal drie jaar waarin gegevens die zijn verzameld door middel van de interceptiebevoegdheid ex artikel 48 van het wetsvoorstel mogen worden bewaard, waarna ze moeten worden vernietigd.

In paragraaf 3.4 staan regels omtrent de interne en externe verstrekking van gegevens die met behulp van bijzondere bevoegdheden zijn verzameld. De interne verstrekking betreft de verstrekking binnen de desbetreffende dienst, waarbij het *need to know*-beginsel centraal staat. Bij de externe verstrekking gaat het om de verstrekking van door de dienst verwerkte gegevens aan externe instanties; deze vormen van verstrekking zijn in paragraaf 3.4.2 (nauwgezet) genormeerd. Ter zake van de samenwerking tussen AIVD en MIVD is in artikel 86, tweede lid, onder a, geregeld dat de diensten onderling gegevens kunnen uitwisselen. Daarnaast is ten behoeve van externe samenwerking een regeling opgenomen inzake de samenwerking met inlichtingen- en veiligheidsdiensten van andere landen (artikelen 88 tot en met 90) waarbij tevens een procedure is vastgelegd die moet worden doorlopen bij het aangaan van samenwerkingsrelaties. De daarvoor geformuleerde criteria dienen steeds in onderlinge samenhang te worden gewogen. Relevante en voor de diensten kenbare factoren, zoals bijvoorbeeld de voor de buitenlandse dienst geldende wet- en regelgeving ter zake van toezicht, eisen omtrent gegevensverwerking en de toegekende bevoegdheden dienen in de te maken afweging te worden betrokken.

Voorzienbaarheid: de toestemmingssystematiek

Dat de waarborgen in het wetsvoorstel zwaarder worden naarmate de inbreuk op de persoonlijke levenssfeer groter is, komt ook tot uiting in de gewijzigde toestemmingssystematiek. Bij de diverse bijzondere bevoegdheden is bepaald welke instantie toestemming dient te verlenen. In zijn algemeenheid geldt dat de uitoefening van een bijzondere bevoegdheid slechts is toegestaan, indien, voor zover niet anders bepaald, de betrokken minister daartoe toestemming heeft gegeven, en nadat deze toestemming van de minister is bekrachtigd met een rechtmatigheidsoordeel door de Toetsingscommissie inzet bevoegdheden (TIB). Het rechtmatigheidsoordeel betreft hier een bindende toets. Het verzoek om toestemming voor de inzet van de bevoegdheden en een verzoek om verlenging daarvan omvatten onder meer het beoogde doel van de uitoefening en de reden waarom de uitoefening van de specifieke bevoegdheid noodzakelijk wordt geacht.

De betrokken minister draagt steeds volledige ministeriële verantwoordelijkheid voor de inzet van bijzondere bevoegdheden door de betreffende inlichtingen- en veiligheidsdienst en is mitsdien gehouden daarover parlementaire verantwoording af te leggen. De rechtmatigheidstoets voorafgaand aan de inzet van de bijzondere bevoegdheid door de

TIB staat aan dit uitgangspunt van de ministeriële verantwoordelijkheid niet in de weg. Het vergelijkend onderzoek naar de wetgeving van andere landen laat op dit punt eenzelfde beeld zien.

De rechtmatigheidsbeoordeling door de TIB is ten opzichte van de huidige Wiv 2002 een verdere versteviging en een nieuw element in het gehele systeem van het toezicht op de inzet van de bijzondere bevoegdheden door de inlichtingen- en veiligheidsdiensten. De bijzondere bevoegdheden van de inlichtingen- en veiligheidsdiensten vragen gelet op hun potentieel inbreukmakend karakter om een adequaat toezichtsysteem, waarvan een bindende onafhankelijke toets voorafgaand aan de uitvoering een onderdeel is. De regering beseft dat de bijzondere bevoegdheden van de AIVD en MIVD diepgaand in kunnen grijpen in de persoonlijke levenssfeer van burgers en een democratische samenleving als zodanig.[188] Dat geldt eens te meer waar het heimelijke karakter van maatregelen in combinatie met gerichte toepassingen in de internet- en communicatietechnologie gemakkelijker dan voorheen kunnen leiden tot graverende inbreuken, waarvan burgers op geen enkele manier weet hebben of zelfs weet kunnen hebben. Steviger toezicht dan voorheen acht de regering om die reden aangewezen. Het EHRM heeft deze mogelijke samenloop van heimelijkheid van de toepassing en de technologische ontwikkelingen ook gesignaleerd in *Szabo en Vissy tegen Hongarije* (2016).[189] In de PIA Wiv is voor de betekenis van deze ontwikkelingen eveneens expliciet aandacht gevraagd.[190] De regering heeft zich naar aanleiding van deze reacties beraden en zag dientengevolge aanleiding om het toezichtsysteem rondom de uitvoering van de bijzondere bevoegdheden opnieuw te doordenken.

Het EHRM heeft zoals hiervoor beschreven in zijn jurisprudentie meermaals benadrukt onafhankelijk toezicht voorafgaand aan en tijdens de inzet van de bijzondere bevoegdheden te eisen. Het heeft daarbij aangegeven dat zijn voorkeur uitgaat naar uitoefening van dat toezicht door de onafhankelijke rechter, maar het EHRM kan ook instemmen met een andere onafhankelijke en onpartijdige toezichthouder mits deze is voorzien van effectieve bevoegdheden om het onafhankelijke toezicht daadwerkelijk adequaat te kunnen uitoefenen. De TIB die de inzet van de bevoegdheden op rechtmatigheid zal beoordelen, is een onafhankelijke en onpartijdige commissie, bemenst met drie personen, waarvan ten minste twee personen zes jaren of meer werkzaam zijn of zijn geweest in een rechterlijk ambt. Met de onafhankelijkheid, de samenstelling, de kwalificatie van de TIB-leden en met de bindende rechtmatigheidstoets is voldaan aan de eisen van het borgen van een onafhankelijke en onpartijdige

[188] EHRM 22 november 2012, *Telegraaf Media Nederland Landelijke Media B.V. en anderen t. Nederland*, par.98.
[189] EHRM 12 januari 2016, *Szabo en Vissy t. Hongarije*, par. 69 – 71.
[190] Zie hoofdstuk 12 van deze Memorie van Toelichting.

beoordeling op enig moment in het proces van de uitvoering van een bijzondere bevoegdheid door de diensten.

Voor de bijzondere bevoegdheden die een grotere inbreuk maken op het privéleven wordt met het instellen van de TIB voorzien in een ten opzichte van de Wiv 2002 aanvullende waarborg. In de volgende gevallen verleent de minister (zonder mogelijkheid van mandaat) de toestemming voor de uitoefening van bijzondere bevoegdheden en wordt deze door de TIB – voorafgaand aan de uitvoering – getoetst:

- DNA-onderzoek gericht op het vaststellen (inclusief verificatie) van de identiteit van personen, alsook voor het verder verwerken van resultaten van DNA-onderzoek (artikel 43);
- verkennen en binnendringen van geautomatiseerde werken en medewerkingsplicht van derden bij de ontsleuteling (artikel 45);
- onderzoek van communicatie met betrekking tot specifieke personen, organisaties en nummers (aftappen, inzet microfoon etc, in artikel 47);
- onderzoeksopdrachtgerichte interceptie (artikel 48);
- onderzoek aan gegevens verkregen uit onderzoeksopdrachtgerichte interceptie, search gericht op interceptie en search gericht op selectie (artikel 49);
- selectie van gegevens en metadata-analyse gericht op het identificeren van personen of organisaties (artikel 50);
- de medewerkingsplicht van de aanbieder van een communicatiedienst bij interceptie (artikel 53);
- het inzetten van de medewerkingsplicht bij de ontsleuteling van gegevens (artikel 57);
- het opvragen van onder meer opgeslagen telecommunicatie van een gebruiker bij een aanbieder van een telecommunicatiedienst (artikel 54);
- ter zake van het observeren en volgen indien het inzet van technische middelen in de woning betreft (artikel 40)
- bij het doorzoeken van besloten plaatsen, het doorzoeken van gesloten voorwerpen, het verrichten van onderzoek aan een voorwerp gericht op het vaststellen van de identiteit indien het doorzoeken van een woning betreft (artikel 42).

Voor het openen van brieven en andere geadresseerde verzendingen is ingevolge artikel 13 van de Grondwet voorafgaande toestemming van de rechter, in casu rechtbank Den Haag vereist (artikel 44). Dit is ook het geval indien de bijzondere bevoegdheden worden ingezet jegens journalisten, waarbij de uitoefening kan leiden tot de verwerving van gegevens inzake hun bronnen of indien deze bevoegdheden worden ingezet jegens advocaten, waarbij de uitoefening kan leiden tot verwerving van gegevens die

betrekking hebben op de vertrouwelijke communicatie tussen een advocaat en diens cliënt (artikel 30, tweede onderscheidenlijk derde lid).

Het vereiste van een voorafgaande toestemming door een onafhankelijke instantie ten aanzien van journalisten vloeit voort uit de uitspraak van het EHRM in de zaak *Telegraaf Media Groep tegen Nederland*, waarin het EHRM heeft geoordeeld dat artikelen 8 EVRM en 10 EVRM (recht op vrije meningsuiting) werden geschonden, omdat 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.[191] De uitspraken inzake het aftappen van advocaten hebben geleid tot de conclusie dat de wetgeving ook ten aanzien van deze beroepsgroep dient te worden voorzien in een voorafgaande toets door de rechtbank Den Haag.[192] In hoofdstuk 3 van deze memorie van toelichting is reeds nader ingegaan op de wijze waarop de regering aan de rechterlijke uitspraken uitvoering geeft.

Voorzienbaarheid: de duur van de toestemming

In artikel 29, eerste lid, 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 een 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[193], in samenhang met de mate waarin deze bevoegdheid inbreuk maakt op de persoonlijke levenssfeer van burgers, zoals bijvoorbeeld bij de interceptie ex artikel 48 van het wetsvoorstel. 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).

Voorzienbaarheid van de verwerking van DNA-gegevens door de diensten

Voor het onderzoeken en opslaan van celmateriaal en het opslaan van DNA-profielen gelden gelet op het gevoelige karakter van dit type persoonsgegevens ingevolge artikel

[191] EHRM 22 november 2012, *Telegraaf Media Groep t. Nederland*.
[192] Rb Den Haag 1 juli 2015 (KG) ELI: RBDH:7436 en in hoger beroep bevestigd door het Gerechtshof Den Haag op 27 oktober 2015, ECLI:NL:GHDHA:2015:2881.
[193] Een dergelijke overweging heeft het EHRM toegestaan, zie EHRM 18 mei 2010, *Kennedy en anderen t. Verenigd Koninkrijk*, par. 161.

43 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 aan voorwerpen gericht op het vaststellen van de identiteit van een persoon (artikel 22, eerste lid, onder c, Wiv 2002). In navolging van de jurisprudentie van het EHRM[194] en de aanbevelingen van de CTIVD[195] 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 43 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 en de verificatie van de identiteit van een persoon (zie nader par. 3.3.4.4.4 van deze toelichting).[196] Het doel van het DNA-onderzoek door de diensten is met het oog op de gevoelige aard van DNA-gegevens strikt afgebakend; DNA-onderzoek gericht op het afleiden van persoonskenmerken uit het genetisch materiaal is niet toegestaan. Toestemming kan vanwege het inbreukmakende karakter alleen door de betrokken minister en na een rechtmatigheidstoets door de TIB worden verleend. Het verzoek wordt steeds aan de eisen van noodzakelijkheid, proportionaliteit en subsidiariteit getoetst.

De vernietigingstermijn van celmateriaal is zo kort mogelijk gehouden (maximaal drie maanden), conform de overweging van het EHRM in het arrest *S. en Marper tegen 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.[197] Indien onderzoek binnen drie maanden niet mogelijk is gebleken, dienen de betrokken minister en de TIB opnieuw toestemming te geven voor een (eenmalige) verlenging van deze termijn, waarbij in het verzoek om verlenging de reden waarom het niet binnen drie maanden heeft kunnen plaatsvinden, expliciet wordt vermeld.

[194] EHRM 4 november 2008, *S. en Marper t. Verenigd Koninkrijk*, par. 99.
[195] CTIVD toezichtsrapport nr. 42, inzake de toepassing van biologisch forensische onderzoeksmethoden door de AIVD, 7 januari 2005.
[196] Van een regeling voor vingerafdrukken is gelet op de beperkte betekenis van de resultaten ervan in de praktijk afgezien, zie par. 3.3.4.4.4 van deze toelichting.
[197] EHRM 4 november 2008, *S. en Marper t. Verenigd Koninkrijk*, par. 120 en 121.

De bewaartermijn van een vervaardigd DNA-profiel bedraagt ten hoogste vijf jaren. De noodzaak van deze termijn is ingegeven door het karakter van veel terroristische misdrijven. Zij ontvouwen zich veelal pas na een langere periode. In de praktijk betekent dat dat bepaalde personen voor langere tijd, soms enkele jaren, uit beeld verdwijnen, maar dat zij op een later moment alsnog in Nederland in beeld komen met het oogmerk om terroristische misdrijven te plegen (zie hiervoor nader paragraaf 3.3.4.4.4).

Na het verstrijken van deze termijn kan op een verzoek van het hoofd van de dienst conform artikel 43, zevende lid, door de minister toestemming worden verleend om de termijn te verlengen met dien verstande dat de bewaartermijn in totaliteit de dertig jaar niet overschrijdt. Het verzoek daartoe dient te voldoen aan de in artikel 29, tweede lid, van het wetsvoorstel gestelde eisen, waaronder het noodzakelijkheidsvereiste. De noodzaak tot verlening kan in een concreet geval ingegeven zijn door het feit dat het bij onderzoek naar een bepaald persoon is gebleken dat deze voor langere tijd uit beeld is verdwijnen, maar dat deze vervolgens alsnog concrete voornemens blijkt te hebben om terroristische misdrijven in Nederland te ontplooien. De minister dient ter zake van de noodzaak van het verlengen van de termijn bij elk verzoek een afweging te maken. De noodzaak van deze bewaartermijn wordt nader toegelicht in paragraaf 3.3.4.4.4 van deze toelichting.

Bij algemene maatregel van bestuur – na een voorhangprocedure bij beide Kamers der Staten-Generaal (artikel 43, achtste lid van het wetsvoorstel) - kunnen nadere regels worden gesteld, onder andere met betrekking tot het verrichten van DNA-onderzoek, het verwerken van DNA-profielen, waaronder begrepen 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 en wordt voorzien in een democratische inbedding.

Indachtig de voorkeur van het EHRM ter zake van een voorafgaande rechterlijke toets vanwege het onafhankelijke en onpartijdige karakter, is met het beoordelen van de rechtmatigheid van een verzoek tot inzet van de inbreukmakende bevoegdheden door de TIB voldaan aan het EVRM. Gelet op het geheel van voornoemde waarborgen komt een balans tot uiting in het wetsvoorstel tussen het belang van een effectieve bescherming van de persoonlijke levenssfeer van burgers en het belang bij een adequate bescherming van de nationale veiligheid voor wat betreft de EHRM-vereisten van de voorzienbaarheid van de maatregelen. Wij menen derhalve dat het wetsvoorstel met deze waarborgen voldoet aan de kwalitatieve vereisten die door het EHRM aan de voorzienbaarheid worden gesteld. De hierboven weergegeven regels en aangescherpte vereisten met

betrekking tot gegevensverwerking en voorafgaande toestemmingverlening voldoen eveneens aan de in het EVRM neergelegde eisen van kenbaarheid en voorzienbaarheid.

Deze waarborgen rondom de legaliteit (de kenbaarheid en de voorzienbaarheid) dienen in samenhang met de hierna te bespreken eisen van noodzakelijkheid, proportionaliteit en subsidiariteit te worden bezien.

EVRM-eisen tan aanzien van 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 ten behoeve waarvan een beperking kan worden gerechtvaardigd. Het belang van de nationale veiligheid is er één van. Het begrip nationale veiligheid in het EVRM behelst een ruime notie. Er is geen sluitende definitie van nationale veiligheid te geven, mede omdat dreigingen van de nationale veiligheid velerlei vormen kunnen aannemen en moeilijk op voorhand zijn te voorzien of meer precies af te bakenen. De contouren van de reikwijdte van het begrip zijn nader uitgewerkt in jurisprudentie van het EHRM.[198] 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.

EVRM-eisen ten aanzien van noodzakelijkheid van de maatregelen in een democratische samenleving

Artikel 8, tweede lid van het EVRM vereist dat beperkingen noodzakelijk zijn in een democratische samenleving. Dit houdt in dat ter rechtvaardiging van de inbreuk op het recht op eerbiediging van de persoonlijke levenssfeer een dringend maatschappelijk belang aanwezig dient te zijn, dat de verwerking van de 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 tegen Duitsland*[199] uit 1978 neemt het EHRM aan dat er in democratische samenlevingen een dringend maatschappelijk belang bestaat bij het

[198] Zie ook het EHRM-rapport *'National security and European case-law'*, November 2013, beschikbaar op http://www.coe.int/t/dghl/standardsetting/dataprotection/judgments_EN.asp. Voorbeelden van een nadere bepaling van het begrip nationale veiligheid zijn te vinden in EHRM 1 juli 2008, *Liberty tegen Verenigd Koninkrijk*, par. 20 en EHRM 18 mei 2010, *Kennedy t. Verenigd Koninkrijk*, par. 159. Het EHRM beoordeelt dit van geval tot geval.
[199] EHRM 6 september 1978, *Klass en anderen t. Duitsland*, par. 48

toestaan van '*secret surveillance*' ten behoeve van de bescherming van de nationale veiligheid. De staat komt volgens vaste jurisprudentie van het EHRM een wat ruimere discretionaire bevoegdheid dan gebruikelijk toe om te bepalen hoe de nationale veiligheid het best kan worden beschermd.[200] Daarbij moet het belang van de staat steeds worden afgewogen tegen het recht op de persoonlijke levenssfeer van haar burgers[201]. 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 steeds moet worden beoordeeld of er geen minder inbreukmakend middel voorhanden is dat even effectief is. Ook dient steeds te worden beoordeeld of is voorzien in toereikende en effectieve waarborgen tegen misbruik van bevoegdheden, die zwaarder moeten zijn naarmate een bevoegdheid meer inbreuk maakt op de persoonlijke levenssfeer.[202]

Noodzakelijkheid, proportionaliteit en subsidiariteit in het wetsvoorstel

In het wetsvoorstel is in diverse onderdelen voorzien in een toets van de noodzakelijkheid, proportionaliteit en subsidiariteit. Ingevolge artikel 18, eerste lid, 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. Ook artikel 28 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 3.2.5 van het wetsvoorstel mag immers slechts worden uitgeoefend voor zover dat noodzakelijk is voor de goede uitvoering van de daarin 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 (waarin de evenredigheid en subsidiariteit beoordeeld dienen te worden) van de inzet van die bevoegdheid te worden aangegeven. Zie daartoe onder meer artikel 29, tweede lid, van het wetsvoorstel.

Tot slot zorgt het afwegingskader dat is neergelegd in artikel 26 van het wetsvoorstel ervoor dat voorafgaand aan elke inzet van een bijzondere bevoegdheid, een belangenafweging wordt gemaakt tussen de door de diensten te behartigen belangen en het belang van de betrokkene. Daarbij moet overeenkomstig artikel 26, eerste lid, worden beoordeeld 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

[200] EHRM 29 juni 2006, *Weber en Saravia t. Duitsland,* par. 104.
[201] EHRM 26 maart 1987, *Leander t. Zweden*, par. 59.
[202] EHRM 18 mei 2010, *Kennedy t. Verenigd Koninkrijk*, par. 153 en EHRM 3 juli 2012, *Robathin t. Oostenrijk*, par. 47-51.

bevoegdheid en dat zij pas daarna, indien dat noodzakelijk blijkt, over mogen gaan tot de inzet van een meer inbreukmakende bevoegdheid.[203] Ook moet in dit kader worden beoordeeld (artikel 26, 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 (artikel 26, vierde lid) 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.

Toezicht gedurende en na afloop van de bevoegdheid

Het EHRM beoordeelt steeds de gehele systematiek van het toezicht die voorafgaand aan en gedurende de uitvoering van de bevoegdheden actief zijn, alsmede de wijze waarop klachtbehandeling van individuele personen is geborgd.[204] Een waarborg tegen misbruik gedurende de uitvoering van de inbreukmakende bevoegdheden bestaat reeds in de Wiv 2002. De regering stelt in het wetsvoorstel voor om de positie van de CTIVD voor wat betreft het toezicht gedurende de uitvoering van de bevoegdheden niet te wijzigen. Deze regeling voldoet aan de vereisten van het EHRM; het gaat het EHRM er immers om dat de toezichthouder gedurende de uitvoering van de bevoegdheden daadwerkelijk toezicht kan houden. De CTIVD had in de Wiv 2002 als toezichthouder passende bevoegdheden toegekend gekregen, waaronder (zelfstandige) toegang tot alle gegevens bij de diensten, de bevoegdheid om onderzoek uit eigen beweging op te starten en verplichte medewerking en de mogelijkheid om personen als getuige of deskundige op te roepen.

De CTIVD is een onafhankelijke toezichthouder. De onafhankelijke bindende toets voorafgaand aan de uitvoering van (bepaalde) bijzondere bevoegdheden door de TIB en het toezicht tijdens de uitvoeringsfase door de CTIVD, wordt in het wetsvoorstel aangevuld in die zin dat de CTIVD tevens als een zelfstandige onafhankelijke klachtinstantie wordt gepositioneerd – in de vorm van een aparte klachtenafdeling bij de CTIVD - met de bevoegdheid om jegens de minister bindende oordelen op klachten te geven. Daarbij is vanwege de eis van onbevooroordeelde oordeelsvorming een strikte scheiding aangebracht tussen de toezichthoudende en klachtbehandelende taak van de CTIVD.

In het wetsvoorstel is de positionering van de CTIVD voor wat betreft toezichthouderschap (paragraaf 7.2 van het wetsvoorstel) alsook die van de

[203] CTIVD rapport nr. 38, p. 56.
[204] EHRM 6 september 1978, *Klass e.a. t. Duitsland*, par. 50; EHRM 29 juni 2006, W*eber en Saravia t. Duitsland*, par. 106; EHRM 18 mei 2010, *Kennedy t. Verenigd Koninkrijk*, par. 153.

klachtbehandeling (paragraaf 7.3) nader uitgewerkt. Op de betekenis van de klachtbehandeling wordt gelet op de eigenstandige regeling van het recht op een effectief rechtsmiddel in artikel 13 EVRM nader ingegaan in paragraaf 9.5.

Ten slotte is in artikel 125 e.v. van het wetsvoorstel een klokkenluidersregeling opgenomen voor personen die betrokken zijn bij de uitvoering van deze wet en de Wet veiligheidsonderzoeken en die een vermoeden van een misstand willen melden. Door het samenstel van de maatregelen die zien op het toezicht in alle fasen van de uitvoering van de bijzondere bevoegdheden (voorafgaand aan de inzet, tijdens de uitvoering en na afloop van de inzet) en op de gegevensverwerking wordt op passende wijze invulling gegeven aan de eisen met betrekking tot waarborgen tegen misbruik die voortvloeien uit artikel 8, tweede lid, van het EVRM.

9.2.2 Toetskader artikel 10 Grondwet

Artikel 10 van de Grondwet beschermt het recht op bescherming van de persoonlijke levenssfeer. 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 ex artikel 10. De grondrechten zoals verwoord in de artikelen 12 en 13 Grondwet worden hieronder voor zover relevant in relatie tot onderhavig wetsvoorstel afzonderlijk besproken. Voor de genoemde grondrechten geldt dat zij onder voorwaarden kunnen worden beperkt in het belang van de nationale veiligheid. In deze paragraaf wordt het wetsvoorstel allereerst getoetst aan artikel 10 Grondwet, waarin de bescherming van de persoonlijke levenssfeer (artikel 10, eerste lid van de Grondwet) en het recht op bescherming van persoonsgegevens (artikel 10, tweede en derde lid van de Grondwet) zijn vastgelegd. Artikel 10, eerste lid van de Grondwet staat de wetgever toe dat deze bij of krachtens de wet beperkingen op het recht op eerbiediging van de persoonlijke levenssfeer stelt. Het toetskader van artikel 10 Grondwet kent een competentie-eis die inhoudt dat een formeelwettelijke basis voor inbreuken op de persoonlijke levenssfeer is vereist. Artikel 10 van de Grondwet biedt de mogelijkheid om de uitwerking daarvan in lagere wet- of regelgeving te regelen. Delegatie is toegestaan. Beperkingen van het grondrecht op privacy zijn toegelaten, mits direct of indirect herleidbaar op een formeel wettelijke grondslag. Het wetsvoorstel biedt conform de grondwettelijke eis, een formeelwettelijke grondslag voor inbreuken op het privéleven. Daarmee wordt eveneens de democratische inbedding van het wetsvoorstel gewaarborgd. Met het wetsvoorstel wordt aan de eis van een formeelwettelijke bevoegdheidsgrondslag in artikel 10, eerste lid, van de Grondwet voldaan.

In artikel 10, tweede lid, van de Grondwet is een expliciete regelingsopdracht vastgelegd voor de overheid om regels te stellen ter bescherming van de persoonlijke levenssfeer in

verband met het vastleggen en verstrekken van persoonsgegevens. In artikel 10, derde lid, 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.

In hoofdstuk 3 van het wetsvoorstel is een vrijwel uitputtende regeling met betrekking tot het verwerken van gegevens, waaronder persoonsgegevens, opgenomen, waarbij tevens is voorzien in enkel specifieke bepalingen inzake de verwerking van persoonsgegevens. Dit hoofdstuk omvat onder meer bepalingen inzake het verzamelen, bewaren, verstrekken en vernietigen van gegevens. Waar het gaat om de verstrekking van gegevens voorziet het wetsvoorstel in hoofdstuk 6 in specifieke bepalingen waar het gaat om de verstrekking van gegevens in het kader de samenwerking met 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. 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 net zoals in de Wiv 2002 in het huidige wetsvoorstel een specifieke regeling inzake kennisneming en correctie voorzien. Daarbij 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.[205] De regering heeft in reactie op dit advies aangegeven dat artikel 48 van de Wiv 2002 (artikel 77 van het wetsvoorstel) aan degene die ingevolge artikel 47 van de Wiv 2002 (artikel 76 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 overeenkomt met een correctierecht, terwijl dit tegelijkertijd recht doet aan de wettelijke plicht tot bronbescherming van de diensten. De regeling is daarmee in overeenstemming met de vereisten van artikel 10, derde lid, van de Grondwet met betrekking tot het recht op inzage en correctie.

9.3 Het recht op bescherming van het huisrecht

[205] Zie *Evaluatie Wet op de inlichtingen- en veiligheidsdiensten 2002. Naar een nieuwe balans tussen bevoegdheden en waarborgen*, p. 164.

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 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. 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 Grondwet 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 kunnen verzetten; er is zowel voorzien in de mogelijkheid van uitstel als afstel van de notificatie.

Het binnentreden van woningen zonder toestemming van de bewoner is – gelet op het heimelijke karakter van de taakuitvoering van de diensten - bij de uitoefening van diverse bevoegdheden voorzien. Zo regelt artikel 42 de bijzondere bevoegdheid tot het doorzoeken van besloten plaatsen, waaronder woningen; indien het woningen betreft dient de minister daarvoor toestemming te geven (artikel 42, vierde lid). In artikel 58 van het wetsvoorstel is in algemene zin een regeling gegeven voor de toegang tot plaatsen, waaronder woningen. Ingeval sprake is van betreden van woningen is de Algemene wet op het binnentreden van toepassing. De grondwettelijk geregelde notificatieplicht (het uitbrengen van een verslag aan de bewoner met de mogelijkheid van uitstel of afstel) is specifiek geregeld in artikel 59 van het wetsvoorstel. Dit samenstel van bepalingen geeft uitwerking aan deze grondwettelijke vereisten. Daarnaast wordt voldaan aan alle vereisten die artikel 8, tweede lid, van het EVRM aan deze bevoegdheid stelt: er is een basis in de wet, de bepalingen zijn voldoende nauwkeurig omschreven, de bovengenoemde waarborgen tegen misbruik 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.

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

Artikel 8, eerste lid, van het EVRM en artikel 13 van de Grondwet beschermen respectievelijk het correspondentiegeheim en het brief-, telefoon- en telegraafgeheim. Voor wat betreft het EVRM geldt het eerder weergegeven toetskader van legitimiteit (kenbaarheid en voorzienbaarheid) en het vereiste van noodzakelijkheid (waarin de afweging van proportionaliteit en subsidiariteit moet worden voltrokken).

Artikel 13 Grondwet 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. Artikel 13 van de Grondwet is door de enorme ontwikkelingen op het gebied van elektronische communicatie in de afgelopen decennia al enige tijd achterhaald. Medio 2014 heeft de regering een voorstel tot wijziging van artikel 13 ingediend.[206] Hoewel dit wetsvoorstel nog niet door het parlement is aanvaard zal in de grondwettelijke toets rekening worden gehouden met de voorgestelde wijzigingen en de gevolgen daarvan voor het (gewijzigde) stelsel van interceptiebevoegdheden.

Artikel 13 Grondwet en 8 EVRM: competentie- en materiële toetscriteria

Het huidige artikel 13 Grondwet stelt eisen in de sfeer van competenties aan inbreuken op enerzijds het briefgeheim en anderzijds het telefoon- en telegraafgeheim. Voor inbreuken op het briefgeheim vereist artikel 13, eerste lid, thans dat deze een basis hebben in een wet in formele zin en dat daarvoor voorafgaand aan het openen 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 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. Daar waar het huidige artikel 13 slechts ziet op bescherming van de brief, de telefoon en de telegraaf, ziet de reikwijdte van artikel 8 EVRM op inhoud van communicatie die via een communicatiemiddel wordt getransporteerd. Artikel 8 EVRM heeft thans voor wat betreft de te beschermen middelen een bredere reikwijdte dan artikel 13 Grondwet. Het is deze beperking van artikel 13 Grondwet die het wetsvoorstel ter zake wil repareren. Het thans aanhangige zijnde artikel 13 Grondwet stelt voor alle inhoud van communicatie, ongeacht met welk communicatiemiddel deze wordt

[206] 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, 16 juli 2014, Kamerstukken 2013/14, 33 989.

overgebracht, aan dezelfde eisen te onderwerpen. Artikel 8 EVRM kent een hiermee vergelijkbare benadering. Artikel 8 EVRM vereist daarnaast middels materiële eisen 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.

Reikwijdte van artikel 13 Grondwet

Artikel 13 van de Grondwet en artikel 8 EVRM beschermen gerichte, niet openbare communicatie, ofwel privécommunicatie, tegen heimelijke kennisneming door anderen dan de verzender of ontvanger. De vertrouwelijkheid van communicatie tussen twee of meer personen, instellingen of organisaties vormt in een democratische rechtsstaat een zwaarwegend belang.[207] Privécommunicatie moet, gelet op het niet-openbare karakter van de inhoud derhalve ook 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 van een vakvereniging, of binnen groepen personen zoals *chats* op een alleen voor leden toegankelijke en daarmee besloten website.[208] Artikel 13 van de Grondwet ziet alleen op bescherming van inhoud van communicatie die door middel van een communicatiemiddel wordt getransporteerd, waarbij een derde belast is met het betreffende transport. In het voorgestelde artikel 13 van de Grondwet valt hieronder, voor zover het gerelateerd is aan het transport, ook de (tussentijdse) opslag. Daarbij kan 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 openbare elektronische communicatiediensten. Zogenaamde onmiddellijke communicatie zoals het onmiddellijke gesprek – waarbij geen communicatiemiddel wordt gebruikt – valt derhalve niet onder de bescherming van artikel 13 van de Grondwet. Deze communicatie wordt beschermd onder artikel 10 van de Grondwet.

De bescherming van artikel 13 van de Grondwet betreft voorts alleen de inhoud van de communicatie. Verkeersgegevens, ofwel metadata, die geen informatie geven over de inhoud maar informatie verschaffen over de overdracht en de opslag van de

[207] Memorie van Toelichting bij het wetsvoorstel tot wijziging van artikel 13 van de Grondwet, Kamerstukken 2013-2014, 33 989, nr. 3, p. 8.
[208] Memorie van Toelichting bij het wetsvoorstel tot wijziging van artikel 13 van de Grondwet, Kamerstukken 2013/14, 33 989. nr 3, p. 15-17.

communicatie, vallen voor zover zij niet de inhoud betreffen buiten het bereik van artikel 13. In die gevallen waarin de metadata de tevens inhoud van de communicatie betreffen, zoals bijvoorbeeld het geval is met de SMS of de onderwerpregel van een e-mail, vallen deze gegevens wel onder de reikwijdte van artikel 13 van de Grondwet. Metadata worden voor zover zij persoonsgegevens betreffen, wel beschermd door artikel 10 van de Grondwet en artikel 8 EVRM.[209] In de praktijk blijkt het steeds lastiger om metadata en inhoud te scheiden.[210] Bijvoorbeeld omdat de onderwerpregel van e-mails informatie geeft over de inhoud van de communicatie. Metadata kunnen mits verwerkt op een voldoende geaggregeerd niveau informatie verschaffen over het privéleven van de betrokkene, zoals over diens communicatiepatroon en over degenen met wie hij in contact staat. Het EHRM liet in zijn uitspraken tot dusverre in het midden of deze gegevens worden beschermd door het algemene recht op privéleven of door het correspondentiegeheim ex artikel 8, eerste lid van het EVRM – de bescherming is in beide gevallen hetzelfde. Het EHRM onderwerpt eventuele inbreuken aan een beoordeling onder de materiële criteria van artikel 8, tweede lid van het EVRM.

Bescherming van het briefgeheim

Artikel 44 van het wetsvoorstel voorziet in een bevoegdheid tot het maken van een inbreuk op het briefgeheim zoals thans vastgelegd in artikel 13 Grondwet. In deze bepaling wordt uitvoering gegeven aan het grondwettelijke vereiste dat voor een dergelijke inbreuk voorafgaande, rechterlijke machtiging is vereist (artikel 44, eerste lid). De door de regering voorgestelde wijziging van artikel 13 van de Grondwet laat ruimte voor een afwijkende regeling. Immers, in de hoofdregel in artikel 13, eerste lid, is de eis van een voorafgaande rechterlijke machtiging weliswaar opgetrokken naar alle vormen van telecommunicatie, inclusief communicatie per post, maar in het betreffende wetsvoorstel is in artikel 13, tweede lid 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 grondwettelijke eis van een voorafgaande rechterlijke machtiging. In zoverre is geen verandering beoogd met de waarborgen die in de Wiv 2002 waren neergelegd. In het kader van waarborgen tegen misbruik is relevant dat de algemene regeling in artikel 59, eerste lid van het wetsvoorstel inzake notificatie van toepassing is op de bevoegdheid tot het openen van correspondentie. Op basis daarvan dient verslag te worden gedaan aan de betrokkene

[209] EHRM 2 augustus 1984, *Malone t. Verenigd Koninkrijk*, par. 64 en EHRM 25 september 2001, *P.G. en J.H. t. het Verenig Koninkrijk*, par. 42.
[210] Rapport Koops en Smits 2013.

van de inbreuk op het briefgeheim, tenzij gronden aanwezig zijn voor uitstel of afstel daarvan.

Bescherming van 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 van alle communicatiemiddelen in de hoofdregel op tot het niveau van het huidige briefgeheim. Op dit moment zijn alle 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[211], telefoon[212] en e-mail, zowel thuis als op het werk[213], maar ook op bescherming tegen het volgen van een persoon via GPS[214], het verzamelen van publieke informatie over een persoon[215], het aftappen van pager berichten[216] en het via de media bekend maken van beelden op bewakingscamera's.[217] Het recht op bescherming van de telecommunicatie is steeds aan de orde bij de artikelen van paragraaf 3.2.5.6 van het wetsvoorstel, dat ziet op onderzoek van communicatie. Het gaat meer concreet om de bevoegdheden tot interceptie van communicatie (gericht dan wel onderzoeksopdrachtgericht), het *searchen* en selecteren van de gegevens die door middel van de onderzoeksopdrachtgerichte interceptie zijn verkregen. De jurisprudentie van het EHRM ter zake van de waarborgen van artikel 8, tweede lid, van het EVRM is op al deze vormen van verwerking van gegevens van toepassing.[218] Artikel 8 EVRM beschermt de telecommunicatie op dezelfde wijze als andere inbreuken op de persoonlijke levenssfeer, door middel van het hierboven uiteengezette toetsingskader onder paragraaf 9.2.

Interceptie van de inhoud van communicatie

Het onderzoek van communicatiegegevens speelt een belangrijke rol in de taken van de diensten. Het verzamelen van gegevens over communicatie en het verwerken van die gegevens leidt vrijwel altijd tot een inbreuk op de persoonlijke levenssfeer van burgers (een uitzondering is militair verkeer, zie de uitzondering van artikel 47, achtste lid). In *M.M. tegen het Verenigd Koninkrijk* stelt het EHRM dat 'the greater the scope of the recording system, and thus the greater the amount and sensitivity of data held and available for disclosure, the more important the content of the safeguards to be applied

[211] Artikel 8, eerste lid, van het EVRM noemt expliciet 'correspondentie'.
[212] EHRM 6 september 1978, *Klass t. Duitsland,* par. 41.
[213] EHRM 25 juni 1997, *Halford t Verenigd* Koninkrijk; EHRM 3 juli 2007, *Copland t. Verenigd Koninkrijk*.
[214] EHRM 2 september 2010, *Uzun t. Duitsland*
[215] EHRM 25 mei 2011, *Association "21 December 1989" en anderen t. Roemenië*.
[216] EHRM 22 oktober 2002, *Taylor – Sabori t. Verenigd Koninkrijk*.
[217] EHRM 28 januari 2003, *Peck t. Verenigd Koninkrijk*.
[218] Zie par. 10.2.1 en CTIVD rapport nr. 38, p. 47-48.

at the various crucial stages in the subsequent processing of the data'.[219] Het EHRM onderkent ten aanzien van interceptie dat een onderscheid bestaat tussen ongericht onderscheppen en gericht onderscheppen van telecommunicatie. Voor wat betreft het wetsvoorstel zijn 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 op de bijzondere bevoegdheden inzake onderzoek van communicatie van toepassing, waaronder begrepen de bepalingen die invulling geven aan de vereisten van noodzakelijkheid, proportionaliteit en subsidiariteit.

Voor wat betreft *gerichte interceptie* van telecommunicatie dient het zware toestemmingsregime van de minister en de rechtmatigheidstoets door de TIB voorafgaand aan de uitvoering van interceptie van de communicatie met betrekking tot specifieke personen, organisaties en nummers dan wel technische kenmerken (waaronder ook de telefoontap valt) te worden gevolgd. Bij dit type interceptie is of zijn concrete personen en/of organisaties in beeld.

Het besluit om over te gaan tot *onderzoeksopdrachtgerichte interceptie* is hoofdzakelijk een beslissing die gebaseerd is op een analyse van de vraag of bepaalde omstandigheden, gebeurtenissen of activiteiten een dusdanige bedreiging opleveren van de nationale veiligheid, dat zij de inzet van dit middel rechtvaardigen. Het EHRM laat aan de nationale autoriteiten een ruime beoordelingsmarge op dit punt, maar het stelt hoge eisen aan de waarborgen waarmee de inzet gepaard gaat. Bij dit type interceptie is elk van de drie stappen in het interceptieproces - de interceptie zelf, de search alsmede de selectie van de opbrengst en de metadata-analyse voor zover gericht op het identificeren van persoon of organisaties – voorafgaand aan de uitvoering toestemming van de minister en een rechtmatigheidstoets door de TIB noodzakelijk. Het onafhankelijk toezicht bij interceptie vormt volgens de jurisprudentie van het EHRM steeds een belangrijke waarborg tegen misbruik.[220] De bevoegdheid tot het verlenen van toestemming kan niet worden gedelegeerd of gemandateerd.

Daarnaast is het stellen van limieten aan de bewaartermijnen van gegevens bij inzet van interceptiebevoegdheden een belangrijke waarborg volgens de jurisprudentie van het EHRM.[221] In artikel 27 van het wetsvoorstel is in algemene zin bepaald dat de gegevens die zijn verkregen door uitoefening van een bijzondere bevoegdheid als bedoeld in paragraaf 3.2.5, derhalve ook door uitoefening van de bevoegdheid tot gerichte interceptie, zo spoedig mogelijk dienen te worden onderzocht op hun relevantie voor het onderzoek waarvoor ze zijn verworven. Gegevens waarvan is vastgesteld dat deze niet

[219] EHRM 13 november 2012, *M.M. t. Verenigd Koninkrijk*, par. 200.
[220] EHRM 29 juni 2006, *Weber en Saravia*, par. 95.
[221] EHRM 29 juni 2006, *Weber en Saravia*, par. 95.

relevant zijn voor het onderzoek dan wel enig ander lopend onderzoek vallend onder de taken als bedoeld in artikel 8, tweede lid, onder a en d, en artikel 10, tweede lid, onder a, c en e, van het wetsvoorstel dienen te worden vernietigd. Gegevens die, tenzij bij de wet anders is bepaald, na een periode van een jaar niet op hun relevantie voor het onderzoek dan wel enig ander lopend onderzoek zijn beoordeeld, dienen te worden vernietigd. Waar het gaat om gegevens die zijn verkregen door middel van de bevoegdheid tot onderzoeksopdrachtgerichte interceptie is een van artikel 27, eerste lid, afwijkende regeling gegeven en geldt een maximale bewaartermijn van drie jaar (artikel 48, vijfde lid).

Ook de specifieke regelingen voor kennisneming van de inhoud van geïntercepteerde gegevens door specifiek daartoe aangewezen ondergeschikte ambtenaren, zoals onder meer voorzien in de artikelen 48, vierde lid en 49, vijfde lid van het wetsvoorstel, geven uitvoering aan het vereiste van het EHRM dat de bevoegdheden met voldoende waarborgen tegen misbruik moeten zijn omkleed.[222] Ten aanzien van de waarborgen tegen misbruik bij gerichte interceptie is nog relevant om te wijzen op artikel 47, vierde lid, van het wetsvoorstel, waarin de procedure is neergelegd in gevallen waarin bij het verzoek om toestemming het nummer[223] 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.[224]

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 bepalingen in het wetsvoorstel die zien op interceptie van communicatie voldoen aan de eisen die artikel 13 van zowel de huidige Grondwet als de eisen die in het wetsvoorstel tot wijziging van artikel 13 Grondwet en artikel 8, tweede lid, van het EVRM daaraan stellen.

9.5 Artikel 13 EVRM: het recht op een effectief en 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

[222] EHRM 29 juni 2006, *Weber en Saravia*, par. 95.
[223] Of het functionele equivalent: technisch kenmerk.
[224] EHRM 3 juli 2012, *Robathin t. Oostenrijk*, par. 47-51.

gewaarborgd door het EVRM, door de staat zijn of worden geschonden, daarover een klacht moet kunnen indienen bij een bevoegde nationale autoriteit.[225] Deze autoriteit moet niet alleen bevoegd zijn om de klacht inhoudelijk te behandelen, maar ook om passend herstel te bieden.[226] 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[227] en effectief, zowel rechtens als in de praktijk.[228] 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 in de zaak *Segerstedt-Wiberg tegen Zweden* geoordeeld dat de autoriteit de bevoegdheid moet bezitten om bindende beslissingen te nemen en om te kunnen bepalen dat verwerkte gegevens worden verwijderd en vernietigd.[229] 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.[230] 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* 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 steeds 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.[231]

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

[225] EHRM 6 september 1978, *Klass tegen Duitsland*, par. 64 en EHRM 26 oktober 2000, *Kudla t. Polen*, par. 157.
[226] EHRM 21 januari 2011, M.S.*S. t. België en Griekenland*, par. 288; EHRM 25 juni 1997, *Halford t. Verenigd Koninkrijk*, par. 64.
[227] 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.
[228] EHRM 13 december 2012, *El-Masri t. "De voormalige Joegoslavische Republiek Macedonie"*, par. 255; EHRM 26 oktober 2000, *Kudła t. Polen*, 30210/96, par. 152.
[229] EHRM 26 maart 1987, *Segerstedt-Wiberg e.a. t. Zweden*, par. 118.
[230] EHRM 26 maart 1987, *Segerstedt-Wiberg t. Zweden*, par. 118..
[231] EHRM 13 december 2012, *De Souza Ribeiro t. Frankrijk*, par. 79; EHRM 26 oktober 2000, Kudła t. Polen, par. 157.

positioneren als een zelfstandige 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 derhalve verplicht aan de oordelen van de CTIVD gevolg te geven (artikel 124, vijfde lid, van het wetsvoorstel) en dient bovendien zowel de afdeling klachtbehandeling als de klager binnen twee weken te informeren over de wijze waarop aan het oordeel van de afdeling klachtbehandeling uitvoering is gegeven. 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 bevoegdheid (artikel 124, vierde lid). De mogelijkheid om een klacht in te dienen is laagdrempelig[232]: 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 120, 121 of 122 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 voldaan.

9.6 Het recht op een eerlijk proces

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. Thans heeft de regering ook een wetsvoorstel in voorbereiding waarbij wordt voorzien in de opname van een recht op eerlijk proces in de Grondwet. Het recht op een eerlijk proces 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, tweede lid, is bepaald dat niet de rechter, maar de minister

[232] Laagdrempeligheid wordt ook door het EVRM vereist, zie *Klass e.a. tegen Duitsland*, par. 36.

beoordeelt of bepaalde processtukken geheim moeten blijven. In het wetsvoorstel wordt de regeling met betrekking tot geheimhouding van processtukken in lijn gebracht met de vereisten van artikel 6 EVRM. Deze regeling wordt besproken hoofdstuk 8 van deze memorie van toelichting. Kortheidshalve wordt daarnaar verwezen.

Hoofdstuk 10 Overzicht van wetgeving in enkele andere landen

10.1 Inleiding

Bij de gelegenheid van de herziening van de Wiv 2002 heeft de regering besloten de wetgeving van een aantal buurlanden op enkele onderdelen te bezien, teneinde de keuzes die in het kader van de herziening van de Wiv zijn gemaakt in een bredere Europese context te plaatsen. De focus in de vergelijking ligt daarbij op de Duitse, de Britse, de Franse en de Belgische wetgeving.[233] In de vergelijking zullen twee onderwerpen worden beschreven, te weten de wijze waarop het toestemmingen- en toezichtsregime in relatie tot inbreuken op de persoonlijke levenssfeer en de onderzoeksopdrachtgerichte interceptie, in enkele landen aangeduid als intercepteren in bulk.
Beschreven wordt op welke wijze de inrichting van het toestemmingenregime in de wet is verankerd, welke instantie(s) betrokken is (of zijn) bij het toezicht tijdens de uitvoering en met welke bevoegdheden zij zijn bekleed, welke rechtsmiddelen in de wet zijn vastgelegd in het geval van een vermeende schending van een (van de) grondrecht(en), en of ten aanzien van de uitvoering van bijzondere bevoegdheden in het buitenland in de wet een rechtsbasis of een specifiek wettelijk toestemmingenregime ter zake is opgenomen.
Ten aanzien van interceptie in bulk wordt voor zover mogelijk weergegeven welk toestemmingsregime geldt, ten aanzien van welke personen bulkinterceptie ingezet kan worden, of ten aanzien van bulkinterceptie in het binnenland en/of buitenland verschillende toestemmings- en toezichtsregimes worden gehanteerd, of onderscheid wordt gemaakt naar kabel- en niet-kabelgebonden interceptie en voor zover van toepassing welke wettelijke bewaartermijnen worden gehanteerd. Ook wordt bezien of in het land een wettelijk vergoedingenregime bestaat ten aanzien van de kosten die aanbieders van telecommunicatienetwerken en –diensten maken om aan hiermee gepaard gaande verplichtingen tegemoet te kunnen komen.
Ter afronding worden enkele vergelijkende observaties weergegeven.
In bijlage 5 bij deze toelichting is een schematische weergave van de wetgeving van enkele landen opgenomen.

[233] Voor de keuze voor de genoemde landen is aangesloten bij de Commissie Dessens, die in haar evaluatie aandacht besteedde aan de vormen van preventief toezicht; zie Evaluatie Wet op de inlichtingen- en veiligheidsdiensten 2002. Naar een nieuwe balans tussen bevoegdheden en waarborgen, p. 94 e.v..

10.2 Duitsland

Duitsland kent drie inlichtingen- en veiligheidsdiensten, te weten het Bundesamt für Verfassungsschutz (hierna: BfV), de Bundesnachrichtendienst (BND) en de Militärischen Abschirmdienst (MAD[234]). In Duitsland zijn de voorschriften en waarborgen ten aanzien van de uitvoering van de bevoegdheden door de verschillende diensten vastgelegd in diverse wetten. Verschillende onderdelen van deze wetten interacteren met elkaar. De G10-wet legt specifiek voorwaarden vast voor beperkingen die betrekking hebben op het 'Brief-, Post- und Fernmeldegeheimnis'.[235] Deze waarborgen bieden bescherming aan Duitse staatsburgers en in beginsel niet-ingezetenen die zich op Duits grondgebied bevinden. In communicatieverkeer in en met het buitenland hebben deze waarborgen beperkte gelding omdat in die gevallen in principe alleen Duitse staatsburgers worden beschermd.

In de regel verleent de Minister van Binnenlandse Zaken of de Minister van Defensie toestemming voor de uitvoering van bijzondere bevoegdheden. In de G10 Gesetz zijn de waarborgen geregeld ten behoeve van personen op het Duits grondgebied, staatsburgers en Duitse belangen in het buitenland. Voor het intercepteren en onderzoeken van telecommunicatie wordt een schriftelijk gemotiveerd verzoek door het diensthoofd of zijn plaatsvervanger ingediend bij de Minister van Binnenlandse Zaken[236] of bij de Minister van Defensie.[237] Wanneer de minister instemt met het verzoek leidt hij het door naar de G-10 commissie voor de rechtmatigheidstoets[238], die bij positieve bevinding door de G10-commissie leidt tot toestemming voor de uitvoering.[239] De toestemmingsduur bedraagt wanneer de G10-commissie betrokken is ten hoogste drie maanden en kan worden verlengd wanneer de procedure opnieuw wordt doorlopen. De G-10 is samengesteld uit een voorzitter die voldoet aan de vereisten die gelden voor de benoembaarheid tot rechter en drie overige leden, die alle worden benoemd[240] door het federaal parlementair controlegremium (*Parlementarisches Kontrollgemium,* hierna: parlementaire gremium) dat een eigen basis heeft in artikel 45 (d) van de Duitse

[234] Artikel 14 MADG regelt de rechtsgrondslag voor de bevoegdheden van de *Militärischen Abschirmdienst* (de MADG heeft geen eigen uitvoerende bevoegdheden, maar op kazernes, in buitenland/missiegebieden heeft zij wel eigen bevoegdheden). De BND en de BfV zijn veruit de meest relevante diensten voor de rechtsvergelijking, derhalve zal de beschrijving van de diensten tot de BND en de BfV worden beperkt.
[235] Bundesambt für Verfassungsschutz (BfV, intern) in art. 8b I-III Bundesverfassungsschutzgesetz (BVerfSchG); artikel 1, tweede lid, Bundesnachrichtendienstgesetz (BNDG); artikelen 9, 10, 14, 15 V-VI van het *Artikel 10-Gesetz* (G-10). Deze bepalingen gelden eveneens voor de Bundesnachrichtendienst en voor de Militärischen Abschirmdienst.
[236] Artikelen 9 en 10 G-10 Gesetz en artikel 8b BVerSchG. Binnen het bestek van dit onderzoek wordt voor Duitsland alleen gekeken naar de bevoegdheden op federaal niveau en wordt dus steeds gesproken over federaal bevoegde autoriteiten.
[237] Voor gevallen waarin de minister van Defensie het verzoek indient, zie artikel 4a MADG jo. 8a, tweede lid, en 2a BervSchG.
[238] Artikel 15, vijfde lid, G-10.
[239] Artikel 15 G-10 Gesetz.
[240] Voor de termijn van één regeringsperiode, daarna worden leden opnieuw benoemd.

Grondwet.[241] De G-10 commissie is geen rechterlijk orgaan, al heeft het *Bundesverfassungsgericht* de G-10 commissie eerder wel gekwalificeerd als gelijkwaardig met een rechterlijk orgaan. Binnen zes maanden na de toestemmingsverlening informeert de minister het eerder genoemde parlementaire gremium over de verleende toestemmingen.[242] Het parlementaire gremium stelt op zijn beurt de Duitse *Bundestag* op de hoogte over de wijze waarop de uitvoering, alsook over de aard en de omvang van de maatregelen die zijn uitgevoerd.[243] Enkel bij onmiddellijk dreigend en ernstig gevaar kan de toestemming hiervoor achteraf worden gevraagd. De G10-Commissie is tevens bevoegd het rechtmatigheidstoezicht gedurende de inzet van de bevoegdheden te verrichten. Indien de G10-Commissie in deze fase een onrechtmatigheid in de uitvoering vaststelt, dient deze onmiddellijk te worden stopgezet. Daarnaast en in aanvulling op het toezicht van de G10-Commissie is een toezichthoudende rol weggelegd voor het parlementaire gremium. Tot slot is het voor burgers mogelijk om tegen de inzet van de bevoegdheden in het bijzonder vanwege een vermeende schending van de persoonlijke levenssfeer, verzameling en verwerking van persoonsgegevens of het communicatiegeheim een klacht in te dienen bij de Duitse bestuursrechter. Dit rechtsmiddel staat echter pas tot de beschikking van de klager nadat deze naar aanleiding van de inzet van een bijzondere bevoegdheid jegens hem een notificatie heeft ontvangen. In deze gevallen staat ook beroep open. In de gevallen waarin iemand (nog) geen notificatie heeft ontvangen maar andere aanwijzingen of vermoedens bestaan dat jegens hem een bijzondere bevoegdheid is of wordt ingezet, kan de klager de G-10 commissie in kennis stellen, of een klacht indienen bij het *Bundesverfassungsgericht*.[244] In het laatste geval dient de klacht een basis te hebben in een schending van één van de grondrechten uit de Duitse Grondwet. Te allen tijde kan een individu bij de diensten informatie opvragen over verwerkte data ten aanzien van hem of haar; tegen een afwijzend besluit kan de bestuursrechtelijke weg worden gevolgd. Ook kan ongenoegen over het gedrag van de inlichtingen- en veiligheidsdiensten worden voorgelegd aan het parlementaire gremium.[245] De minister is steeds politiek verantwoordelijk voor de uitvoering van de bevoegdheden. Doordat de beoordeling van de voorafgaande toestemming, het toezicht gedurende de inzet van

[241] De commissie Dessens stelt in haar evaluatie dat de G-10 commissie in zekere zin kan worden beschouwd als een vorm van gedelegeerde parlementaire controle (evaluatie. P. 96). De band komt ook tot uitdrukking door het feit dat de G-10 commissie leden zitten gedurende een regeringsperiode, daarna worden zij vervangen (of herbenoemd).
[242] Artikel 14, eerste lid, Kontrollgremiumgesetz (PKGrG).
[243] Het gaat om maatregelen die zijn genomen ex artikel 3 (interceptie gericht op targets), 5 (bulkinterceptie), 7a (onderzoek op plaatsen in het buitenland) en 8 G10-Gesetz (bedreigde personen in het buitenland).
[244] De wettelijke notificatieplicht regelt dat in beginsel altijd wordt genotificeerd, maar dat deze tot maximaal 12 maanden kan worden uitgesteld. Indien notificatie langer wordt uitgesteld dient dit te worden medegedeeld aan de G-10 commissie. Deze kan maximaal vijf jaren na beëindiging van de inzet van de bevoegdheid besluiten dat de notificatie definitief achterwege blijft. In het kader van de inzet van bevoegdheden ten aanzien van passagiersgegevens en rekeninggegevens bij kredietinstituten is afstel van notificatie uitgesloten.
[245] Artikel 8, tweede lid, PKGrG.

bevoegdheden en achteraf alsmede de klachtbehandeling sequentieel plaatsvindt, bestaat in beginsel ruimte om de besluitvorming die in een vorige fase heeft plaatsgevonden, te heroverwegen.

De Duitse wetgeving kent geen nader afwegingskader ter zake van de inzet van bijzondere bevoegdheden in of over het buitenland. In dienstvoorschriften zijn voor de *Bundesnachrichtendienst* ter zake van de uitvoering van bevoegdheden (waaronder bulkinterceptie in het buitenland) de procesmatige voorwaarden vastgelegd. In 2001 is de Duitse wetgeving aangepast om bulkinterceptie op de kabel mogelijk te maken. De BND is sindsdien bevoegd om ten behoeve van tijdige onderkenning van bepaalde risico's in bulk te intercepteren.[246] Interceptie kan daarbij gericht zijn op het binnenland in verband met onderzoek naar persoonsgegevens en/of inhoud van ingezetenen of van zich in Duitsland ophoudende communicerende personen (niet-ingezetenen die zich op Duits grondgebied bevinden). Enkel de BND is bevoegd om communicatie van zowel ingezetenen als van niet-ingezetenen die zich op Duits grondgebied bevinden, te onderzoeken. De BfV is bevoegd om gericht te intercepteren.

Voor zover het bulkinterceptie van binnenlands verkeer betreft, dat wil zeggen bulkinterceptie gericht op communicatie van ingezetenen dan wel op niet-ingezetenen die zich op Duits grondgebied bevinden, geldt het G10-regime. Voor bulkinterceptie van buitenlands verkeer, dat wil zeggen interceptie die *niet* ziet op communicatie van Duitse staatsburgers, geldt de algemene regeling ex artikel 1, eerste lid BNDG; hier geldt het G10-waarborgenregime niet.[247]

De BND dient voor de voorgenomen bulkinterceptie in het binnenland een verzoek in bij de minister; het verzoek behelst zoektermen (bijvoorbeeld een bepaald type verkeersgegeven of een term die gerelateerd is aan inhoud) en wijst een regio aan, alsook het percentage van de totale hoeveelheid van de communicatie die over het communicatiekanaal verloopt dat de BND wil binnenhalen.[248] De toestemming geldt voor een duur van maximaal drie maanden.[249] De G10-Commissie behoeft voorafgaand aan bulkinterceptie in het binnenland niet om toestemming te worden gevraagd. Zij treedt wel op als toezichthouder gedurende de interceptie.[250] Buiten dit raamwerk mogen de

[246] Artikel 1, tweede lid, BNDG. Het betreft de zgn. '*Strategische Fernmeldeaufklaerung'*, FmA. De BfV is bevoegd om gericht te intercepteren.
[247] Artikel 1, tweede lid, BNDG luidt: 'Der Bundesnachrichtendienst sammelt zur Gewinnung von Erkenntnisse über das Ausland, die von aussen- und sicherheitspolitischer Bedeutung für die Bundesrepublik Deutschland sind, die erforderlichen Informationen und wertet sie aus. Werden dafür im Geltungsbereich dieses Gesetzes Informationen einschliesslich personenbezogen Daten erhoben, so richtet sich ihre Erhebung, Verarbeitung und Nutzung nach den [artikelen] 2 tot 6 en 8 tot 11 [van de BNDG]'.
[248] Meer dan 20% intercepteren van het totaal van hetgeen aan communicatie via een telecommunicatienetwerk verloopt is wettelijk niet toegestaan, zie artikel 10, vierde lid, G10-Gesetz.
[249] Artikel 10, vijfde lid, G10-Gesetz.
[250] Artikel 15, vijfde en zesde lid, G10-Gesetz.

persoonsgegevens van Duitse staatsburgers, ook van Duitse staatsburgers die zich in het buitenland bevinden, niet ten behoeve van interceptie in bulk worden verwerkt.[251]

Voor interceptie van internationale telecommunicatieverbindingen (dit betreft verbindingen waarbij oorsprong en/of bestemming zich in het buitenland bevinden) verleent de minister toestemming, waarbij het eerdergenoemde parlementaire gremium de minister vooraf toestemming dient te geven bij het bepalen van het telecommunicatienetwerk dat in dat concrete geval dient te worden geïntercepteerd.[252] In beginsel geldt bij interceptie van zowel een nationaal alsook een internationaal netwerk een verbod om zoektermen te gebruiken die identificatiekenmerken of de kern van de persoonlijke levenssfeer betreffen. Dit verbod geldt echter niet voor zover kan worden uitgesloten dat de aansluitingen in het te intercepteren telecommunicatienetwerk niet van Duitse ingezetenen zijn (of niet regelmatig door Duitse ingezetenen worden gebruikt).[253] In de Duitse wetgeving is voor bulkinterceptie inzake het buitenland geen bewaartermijn opgenomen. Tot slot dient de Duitse overheid de telecommunicatiedienstaanbieders tegemoet te komen in de kosten die zij maken met het oog op de technische aanpassingen en overige maatregelen ten behoeve van de taakuitvoering van de diensten.[254] De hoogte van de vergoeding is in beginsel te ijken aan een vast schema van bedragen.[255]

10.3 Verenigd Koninkrijk

Het VK kent een aantal inlichtingen- en veiligheidsdiensten waarvan in het kader van de vergelijking de Security Service, Secret Intelligence Service, Defence Intelligence en de Government Communications Headquarters (GCHQ) het meest in het oog springen. GCHQ is de belangrijkste speler als het gaat om bulkinterceptie. Onder de huidige wetgeving geeft een minister toestemming voor de inzet van bijzondere bevoegdheden, de zgn. 'special powers'. Onder 'special powers' worden in elk geval de inzet van technische middelen en (bulk)interceptie begrepen. Thans is in het Verenigd Koninkrijk een wetsherziening in voorbereiding (de Draft Investigatory Powers Bill) die onder meer tot doel heeft de thans versnipperde wetgeving onder te brengen in één overkoepelende wet. Zo worden onder meer de bevoegdheden gemoderniseerd de toestemmingverlening herzien en verstevigd. Het toezicht wordt vereenvoudigd en verstevigd en een

[251] De voorwaarden voor de verwerking van deze persoonsgegevens (van ingezetenen) zijn vastgelegd in artikel 5 e.v. G10-Gesetz.
[252] Artikel 5, eerste lid, G10-Gesetz.
[253] Artikel 5 G10-Gesetz. Bij de besluitvorming met betrekking tot de inzet van de bevoegdheden dient de BND weliswaar te voldoen aan de beginselen van de grondwettelijke ordening, waartoe het proportionaliteitsbeginsel, het willekeurverbod, het vereiste van wetmatigheid en respect voor menselijke waardigheid behoren. Tot de menselijke waardigheid wordt ook een 'onaantastbare kern van de persoonlijke levenssfeer' gerekend, die eenieder tegen de inzet van de bevoegdheden beschermt.
[254] Artikel 20 G10-Gesetz.
[255] Artikel 23 Justizvergütungs- und –entschaedingungsgesetz (JVEG) jo. bijlage 3 bij artikel 23 JVEG.

beroepsmogelijkheid wordt in de klachtprocedure geïntroduceerd.[256] *Hieronder zal de huidige wetgeving beknopt worden weergegeven, waarna een uitwerking van het wetsvoorstel volgt.*

Onder de huidige wetgeving beoordeelt de Minister van Binnenlandse Zaken verzoeken afkomstig van de S*ecurity Service*; de Minister van Buitenlandse Zaken beoordeelt verzoeken van de *Secret Intelligence Service* en van GCHQ.[257] Ten aanzien van *Defence Intelligence* verleent de Minister van Defensie toestemming. Toestemmingsverleningen kunnen worden verlengd. De huidige wetgeving kent geen onafhankelijke instantie die toetst of de voorgenomen inzet van een bijzondere bevoegdheid een inbreuk maakt op de persoonlijke levenssfeer, of een vergelijkbaar recht. De rechtsbasis voor de toestemmingverlening is op dit moment te vinden in artikel 8 Regulation of Investigatory Powers Act (RIPA) voor wat betreft interceptie, artikel 9 van de Telecommunications Act voor wat betreft het verwerven van metadata en de artikelen 5 en 7 van de Intelligence Services Act (ISA) voor wat betreft de inzet van technische middelen (*equipment interference*). Ingevolge artikel 6, vierde lid, van de Intelligence Services Act (ISA) wordt een verleende toestemming thans ingetrokken indien de inzet van de betreffende technische middelen niet langer noodzakelijk en/of proportioneel is.[258]

Met de voorgenomen wetswijziging wordt voorzien in een proces van toestemmingsverlening waarin in een '*double lock*' is voorzien. Na beoordeling en ondertekening van een verzoek door de minister zal in de nieuwe situatie een *judicial commissioner* een rechtmatigheidstoets verrichten. Daarmee komt de toestemming tot stand en kan de bevoegdheid worden uitgevoerd.[259] Voor wat betreft verzoeken die het opvragen van metadata ('*communications data*') betreffen, wordt het eerdergenoemde '*double lock'* niet geactiveerd. Een verzoek vanuit de diensten tot verkrijging van metadata wordt aan een s*ingle point of contact* gezonden, dat een kwaliteitscontrole verricht. Na goedkeuring wordt het verzoek verzonden naar een '*designated person'* (minimaal een '*senior official'*) die geen betrokkenheid heeft bij het voorgenomen onderzoek. Deze laatste autoriseert het opvragen van metadata.

De *Interception of Communications Commissioner* (ICC) is thans bevoegd toezicht uit te oefenen op de uitvoering van de bijzondere bevoegdheden waarvoor de minister toestemming heeft verleend ter zake van interceptie van post en telecommunicatie

[256] Zie voor Draft Investigatory Powers Bill: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/473770/Draft_Investigatory_Powers_Bill.pdf, p. 5-7 (website bezocht op 23 februari 2016).
[257] Artikel 3 ISA.
[258] Artikelen 2 (Security Services) en 4 (GCHQ) ISA.
[259] Draft Investigatory Powers Bill.

onder de RIPA en artikel 94 van de Telecommunications Act.[260] De ICC wordt benoemd door de premier en heeft conform art 57, vijfde lid, van de RIPA de rang van *high judicial officer*, ofwel dient te voldoen aan de eisen voor benoembaarheid tot rechter. De ICC heeft steeds volledige toegang tot informatie. De toezichthoudende taak van de ICC strekt niet zover dat deze de inzet van een bevoegdheid kan doen schorsen of staken.[261] Naast de ICC kent het Britse toezichtstelsel een *Intelligence Services Commissioner* (ICS). Deze heeft aanvullende taak op het toezicht van de ICC[262] en houdt toezicht op de uitoefening van bijzondere bevoegdheden die zich niet in het toezichthoudend pakket van de ICC bevinden. Het *Intelligence and Security Committee* (dit is samengesteld uit leden van het Hoger- en Lagerhuis) onderzoekt de uitgaven, de beheersing en het beleid van de inlichtingen- en veiligheidsdiensten en van GCHQ.[263] De wetswijziging zal hier een vereenvoudiging aanbrengen; de huidige commissarissen worden verenigd in de *Investigatory Powers Commissioner*. Zijn bevoegdheden zullen worden versterkt: wanneer de IPC in zijn onderzoek vaststelt dat ten aanzien van een persoon op onrechtmatige wijze onderzoek is verricht, kan hij de betrokkene daarover notificeren. Uit het midden van de IPC worden *judicial officers* betrokken die de toestemming verlenen (in het eerdergenoemde '*double lock*'). De IPC zal als toezichthouder vooralsnog niet de bevoegdheid toekomen om tijdens de uitvoering van de bevoegdheden in te grijpen.

Het *Investigatory Powers Tribunal* (IPT) behandelt klachten omtrent het handelen van de diensten. Het IPT bestaat uit minimaal drie leden en is onafhankelijk. De leden dienen aan de eisen tot benoembaarheid als rechter te voldoen, of te voldoen aan een andere wettelijke, gelijkaardige kwalificatie dan wel gedurende tien jaren als advocaat te hebben gefunctioneerd.[264] Met het IPT is thans voorzien in een effectief rechtsmiddel voor eenieder die meent slachtoffer te zijn van een onrechtmatige inzet van de bevoegdheden zoals vastgelegd in RIPA of van een schending van zijn fundamentele rechten en vrijheden zoals vastgelegd in de Human Rights Act (1998) in de zin van artikel 13 van het EVRM. Een klacht dient binnen een jaar na de vermeende onrechtmatigheid onder de aandacht van het IPT te worden gebracht. Thans is het niet mogelijk om tegen een beslissing van het IPT beroep in te stellen.[265] Het is de bedoeling met de wetswijziging een beroepsmogelijkheid wordt gecreëerd bij het *Court of Appeal* in het geval het IPT zelf van oordeel is dat er nog rechtsvragen resteren die een beroep kunnen rechtvaardigen. Indien het IPT daarvan niet overtuigd is, zal deze beslissing

[260] Artikel 8, derde lid ISA regelt de omvang van het toezicht, het vierde lid regelt de medewerkingsplicht van de diensten om de Commissioner van informatie te voorzien en leden 5 en 6 bepalen bevatten bepalingen over verlichte jaarlijkse rapportage aan het parlement.
[261] Artikel 57, tweede lid, RIPA.
[262] Artikel 59 RIPA.
[263] Artikel 10 ISA.
[264] Zie ook Schedule 3 bij RIPA.
[265] Artikel 9, vierde lid, ISA.

finaal zijn en zal beroep niet mogelijk zijn. Artikel 67, tweede lid RIPA schrijft thans voor dat het IPT bij de uitoefening van zijn taak in de klachtprocedure daarvoor dezelfde beginselen en uitgangspunten gelden als in een rechterlijke procedure. De dienst waarvan het handelen wordt onderzocht is wettelijk verplicht om het IPT te voorzien van alle door het IPT gewenste informatie.[266]

De Intelligence Services Act (ISA) regelt de toestemmingverlening voor de inzet van de bevoegdheden in het buitenland. Met 'buitenland' wordt hier bedoeld '*any act outside the British Islands'*. De betrokken minister verleent hiervoor toestemming indien de inzet van bijzondere bevoegdheden in het buitenland effectief, noodzakelijk en proportioneel is. Voor wat betreft bulkinterceptie ten aanzien van buitenlandse communicatie wordt toestemming door het diensthoofd verleend.[267] Indien zich in de in bulk geïntercepteerde communicatie gegevens bevinden van een persoon die zich in het Verenigd Koninkrijk (*British Islands*) bevindt, dient op dit moment indachtig artikel 16, derde lid, RIPA een nadere toestemming (*further warrant*) te worden verkregen wanneer toegang tot de inhoud van de communicatie wordt gewenst. De toestemmingverlening voor verzoeken om bulkinterceptie is thans belegd bij de betrokken minister.

In het wetsvoorstel ter herziening van de RIPA is een nieuw raamwerk voor bulkinterceptie opgenomen. Bulkinterceptie zal in de toekomst enkel mogelijk zijn in het kader van de taken van de inlichtingen- en veiligheidsdiensten (nu kunnen ook politiediensten hier nog gebruik van maken). Elk verzoek dient alsdan te worden getoetst aan eisen van noodzaak en proportionaliteit en bulkinterceptie kan voor wat betreft inhoudelijke communicatie enkel worden ingezet als het doel van de bulkinterceptie is het verwerven van informatie over personen die zich buiten het Britse territorium bevinden. Indien bij de diensten behoefte bestaat aan vergaring van informatie over personen die zich op het Britse grondgebied bevinden, is dat indachtig het wetsvoorstel straks enkel toegestaan indien dat noodzakelijk is ter vervulling van een tevoren bepaald doel. Voordat toegang wordt verkregen tot de verzamelde data dient door de betrokken analisten te worden onderzocht of daarmee voldaan wordt aan de voorwaarden waaronder de toestemming eerder is verleend. Wanneer ook de inhoud van de communicatie van Britse ingezetenen moet worden onderzocht is onder voorgestelde wetgeving een gerichte last noodzakelijk. De minister dient in deze gevallen en in het geval waarin informatie dient te worden vergaard over personen die zich binnen het Britse grondgebied bevinden, toestemming te verlenen binnen het '*double lock'*; de *Judicial Commisioner* zal dan na de minister een toets verrichten. In het wetsvoorstel zijn geen bewaartermijnen voor bulkinterceptie opgenomen; data kan

[266] Artikel 68, zesde lid, RIPA.
[267] Met 'buitenlandse' communicatie wordt communicatie bedoeld die verzonden of ontvangen is buiten het grondgebied van de Britse eilanden, zie artikel 20 RIPA.

worden bewaard zolang als noodzakelijk en proportioneel. Tot slot bepaalt het huidige artikel 14 RIPA dat de minister garant zal staan voor een '*fair contribution*' aan de kosten die post- en telecommunicatiedienstaanbieders wegens het optuigen en in stand houden van een permanent systeem om interceptie mogelijk te faciliteren, moeten maken.[268]

10.4 Frankrijk

In Frankrijk zijn diverse diensten op het terrein van inlichtingen en veiligheid actief, zoals DGSE (Defensie, inlichtingendienst buitenland, vergelijkbaar met SIS in het VK); DRM (een militaire inlichtingendienst) en DPSD (militaire veiligheidsdienst). DGSI (binnenlandse veiligheidsdienst) valt onder het ministerie van Binnenlandse Zaken. In 2015 is de wetgeving, de Code de la Sécurité intérieure, grondig herzien en gemoderniseerd. De waarborgen ter zake van toestemming en toezicht gelden voor bevoegdheden op Frans grondgebied; indien bevoegdheden worden ingezet in het buitenland zijn waarborgen veel minder stringent.

Het juridisch raamwerk, onder meer voor wat betreft de inzet van bijzondere bevoegdheden en het toezicht daarop, is neergelegd in de Code de la Sécurité intérieure (CSI), die laatstelijk is herzien in 2015. De premier geeft steeds toestemming voor de inzet van een bevoegdheid na ontvangst van het advies van de CNCTR (*Commission nationale de controle des techniques de renseignement*).[269] De CNCTR dient alleen vooraf om advies te worden gevraagd in de gevallen waarin op Frans grondgebied op het recht op respect voor de persoonlijke levenssfeer, in het bijzonder het briefgeheim, de bescherming van persoonsgegevens en het huisrecht, een inbreuk zal worden gemaakt.[270] Dit advies strekt zich uit tot de inzet van alle bijzondere bevoegdheden. Hoewel de herziene CSI van 24 juli 2015 oorspronkelijk tot doel had de CNCTR bevoegd te verklaren advies te verlenen voorafgaand aan de uitvoering van de bevoegdheden in het buitenland, oordeelde de *Conseil constitutionnel* in zijn toets voorafgaand aan de inwerkingtreding van de herziene CSI dat het gelet op de afwezigheid van rechtsmacht buiten het Franse territorium niet mogelijk is dat CNCTR ex ante adviseert.[271] Conform

[268] Artikel 24 RIPA kent eenzelfde bijdrageplicht voor de overheid voor wat betreft het meewerken door de post- en telecommunicatiedienstaanbieders aan de wettelijke plicht tot het verzamelen of openbaren van verworven informatie. Artikel 52 RIPA ziet op een bijdrage van overheidswege in de kosten die worden gemaakt door telecommunicatiedienstaanbieders voor wat betreft het openbaren van geëncrypteerde informatie. DRIPA verplicht telecommunicatiedienstaanbieders tot het opslaan van relevante communicatiegegevens. De Minister kan ingevolge artikel 1, derde lid, jo vierde lid sub g DRIPA ter zake regelgeving tot stand brengen, in het kader waarvan ook het vergoeden van de door de aanbieder(s) gemaakte kosten een onderdeel kan zijn. Telecommunicatiedienstaanbieders zijn ingevolge artikel 94, zesde lid Telecommunications Act verplicht gevolg te geven aan de bevelen van de minister voor wat betreft de nationale veiligheid. Het in voorbereiding zijnde wetsvoorstel zal deze separate regelingen in één wet samenbrengen. Aan de vergoedingsverplichtingen van de minister en de verplichting tot medewerking verandert in principe overigens niets.
[269] Artikel 821-1, Code de la Sécurité intérieure, versie 18 februari 2016 relative au renseignement (1) (hierna: CSI) jo. Artikel 833-1.
[270] Artikel 801-1 CSI.
[271] Besluit van het Conseil constitutionnel no. 2015-713 van 23 juli 2015.

het dictum van de *Conseil constitutionnel* geeft de Franse premier voorafgaand aan de uitvoering van bijzondere bevoegdheden in het buitenland toestemming.[272]

De CSI regelt uitdrukkelijk dat de waarborgen rondom de besluitvorming en de uitvoering van de bijzondere bevoegdheden, waaronder de toezichthoudende rol van de CNCTR, enkel worden geactiveerd wanneer de bevoegdheid op Frans grondgebied wordt ingezet.[273] De premier kan gemotiveerd van het advies van de CNCTR afwijken.[274] In spoedeisende gevallen kan toestemming worden verleend zonder voorafgaand advies, al dient het besluit onverwijld en binnen maximaal 24 uren aan CNCTR te worden voorgelegd.[275]

De CNCTR bestaat uit negen leden (twee afgevaardigden, twee senatoren, twee leden van de *Conseil d'État*, twee rechters van het *Cour de Cassation* en een vertegenwoordiger van ARCEP (*Autorité de régulation des Communications et des Postes*). De voorzitter van de CNCTR wordt benoemd conform artikel 13 van de Franse Grondwet - na advies van de permanente parlementaire commissie veiligheid - door de Franse president. Leden worden benoemd voor zes jaar. De CNCTR is een onafhankelijke commissie.

De CNCTR vervult tevens de rol van toezichtsorgaan. Zij heeft daartoe permanent toegang tot alle informatie en ontvangt alle informatie met betrekking tot alle verleende toestemmingen voorafgaand aan de uitvoering en ontvangt voor het overige alle informatie waarom zij verzoekt.[276] De wet legt een actieve informatieplicht vast voor de ministers en alle betrokken autoriteiten; belemmering van de taakuitvoering van CNCTR wordt bedreigd met een boete of met gevangenisstraf.[277] Zij kan zich op elk moment met een aanbeveling over onderbreking of stopzetting van een bijzondere bevoegdheid en/of vernietiging van verzamelde gegevens wenden tot de bij de uitvoering betrokken instanties, inclusief de premier en de betrokken minister. Zodra een aanbeveling wordt ontvangen, informeert de premier de CNCTR onmiddellijk over de wijze waarop uitvoering wordt gegeven aan de aanbeveling. Wanneer de premier geen of onvoldoende gevolg geeft aan de aanbevelingen van de commissie, kan de voorzitter danwel drie leden van de CNCTR de *Conseil d' État* informeren. Jaarlijks rapporteert de CNCTR aan het parlement over haar werkzaamheden.

[272] Artikel L854-1 tot en met L854-9 CSI.
[273] Artikel 801-1, tweede zinsnede.
[274] Artikel 821-4 CSI.
[275] Artikel 821-5 CSI.
[276] Artikel 833-2 CSI.
[277] Artikel 833-3 CSI.

Een ieder kan zich tot de CNCTR wenden met het verzoek te controleren of tegen hem op legitieme wijze middelen worden of zijn ingezet.[278] De CNCTR deelt verzoeker mede dat hij een en ander heeft geverifieerd en niet of er daadwerkelijk middelen zijn of worden ingezet. Een klacht kan in Frankrijk worden ingediend bij de *Conseil d'État* (Raad van State).[279] De CNCTR kan tijdens uitoefening van het toezicht tijdens de uitvoering tot het voortschrijdend inzicht komen dat het eigen advies voorafgaand aan de uitvoering van de bevoegdheid aanleiding geeft tot heroverweging, maar een totaal afwijkende opvatting ligt hier niet voor de hand. De CNCTR zal bij de toezichtuitoefening eerder pragmatisch omgaan met dergelijke voortschrijdende inzichten.

De DGSE is bevoegd om te intercepteren in bulk gericht op internationaal telecommunicatieverkeer.[280] De toestemming ter zake is geldig voor onbepaalde tijd. De premier wijst met een gemotiveerd besluit de telecommunicatienetwerken aan waarop de verwerving wordt toegestaan. Doel moet zijn de verdediging of bevordering van de fundamentele belangen van de staat. Hieronder vallen in ieder geval nationale onafhankelijkheid, territoriale integriteit, nationale defensie, belangen buitenlandpolitiek, economische, industriële en wetenschappelijke belangen, voorkomen terrorisme, voorkomen (georganiseerde) criminaliteit. Vervolgens kan de premier (of een gedelegeerd persoon) op grond van artikel 854-2-II CSI op basis van een gemotiveerd verzoek van een minister (of een gedelegeerd persoon) toestemming geven voor de verwerving van metadata. In het geval van bulkinterceptie van internationaal telecommunicatieverkeer met bestemming en oorsprong in het buitenland geldt een brede interceptiebevoegdheid (bijvoorbeeld op geografische zone, organisatie, groepering of persoon). De toestemming van de premier ter zake van bulkinterceptie gericht op internationaal communicatieverkeer is geldig voor onbepaalde tijd. De premier wijst met een gemotiveerd besluit de telecommunicatienetwerken aan waarop de verwerving van internationaal communicatieverkeer wordt toegestaan. Deze goedkeuring van de premier kan niet worden gedelegeerd. Voor wat betreft bewaartermijnen kunnen buitenlandse communicatiedata (inhoud) tot maximaal vier jaar na ontvangst worden bewaard. Metadata kan tot maximaal zes jaar na ontvangst worden bewaard. Versleutelde data kan maximaal acht jaren worden bewaard.

De Code de la Sécurité intérieure voorziet niet expliciet in de verdeling van de kosten die (openbare) telecommunicatienetwerk- en/of dienstaanbieders verplicht moeten maken. De overheid komt de aanbieders tegemoet met een redelijke vergoeding.

10.5 België

[278] Artikel 833-4 CSI.
[279] Artikel 801-1, vijfde lid jo. Art. 773-1 CSI.
[280] Artikel L854-1 CSI

In België bestaan twee diensten die zich voor wat betreft taken en bevoegdheden laten vergelijken met de Nederlandse inlichtingen- en veiligheidsdiensten, te weten de Veiligheid van de Staat (civiel) en de Algemene Dienst Inlichtingen en Veiligheid (ADIV, militair). Deze diensten oefenen hun bevoegdheden uit in het kader van de Wet bijzondere inlichtingenmethoden 2010[281] en de Wet houdende regeling van de inlichtingen- en veiligheidsdienst (W.I en V) uit 1998.[282] De diensten hebben drie typen bevoegdheden tot hun beschikking: de gewone, de specifieke en de uitzonderlijke methoden, die oplopend een potentieel meer graverende inbreuk op privacy maken. De wetgeving kent geen regeling van een toestemmingverlening ter zake van de inzet van de bevoegdheden van de diensten in het buitenland.

De minister dient toestemming te geven voorafgaande aan de uitvoering van de uitzonderlijke bevoegdheden. De BIM-commissie (vernoemd naar de Wet bijzondere inlichtingenmethoden) voert vooraf een rechtmatigheidstoets uit en het advies is bindend. Een positief advies van de BIM-Commissie geldt voor de duur van twee maanden[283] en kan worden verlengd na het doorlopen van de toestemmingsprocedure. Voor de gewone en de specifieke bevoegdheden verleent het diensthoofd toestemming; daarbij dient het diensthoofd de BIM-commissie vooraf te informeren. Indien de BIM-commissie achteraf vaststelt dat de toestemming door het diensthoofd onrechtmatig is gegeven, mag de data niet worden gebruikt. De BIM-commissie bestaat uit drie leden en drie plaatsvervangende leden die worden benoemd bij koninklijk besluit, na besluit in de Ministerraad op voorstel van de Ministers van Binnenlandse Zaken en Defensie. De BIM-commissie is een onafhankelijke commissie waarvan de leden alle voldoen aan de vereisten die gelden voor de benoembaarheid tot rechter (in elk geval één onderzoeksrechter en één lid dat lid is van het openbaar ministerie; de voorzitter van de BIM-commissie is de onderzoeksrechter). In zeer urgente gevallen dient het diensthoofd positief advies van de BIM-Commissie te verkrijgen waarbij kan worden volstaan met de instemming van de voorzitter.[284] Deze toestemming duurt maximaal 48 uur.

Het toezicht op de uitvoering van de gewone, de specifieke en de uitzonderlijke bevoegdheden wordt uitgeoefend door het Vast Comité op de Inlichtingendiensten (hierna: VCI).[285] Het betreft bindend rechtmatigheidstoezicht. De voorzitter en de leden van het VCI worden benoemd door de Senaat voor een – vernieuwbare - termijn van zes jaar. Voor elk van hen worden ook twee plaatsvervangers benoemd. De voorzitter moet voldoen aan de vereisten die gelden voor de benoembaarheid tot rechter. Het VCI is

[281] Wet op bijzondere lichtingenmethoden van 4 februari 2010 (Wet bijzondere methoden).
[282] Wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdienst (Organieke Wet 1998), hierna: W.IenV.
[283] Artikel 18/10, eerste lid, tweede zinsnede W.I enV.
[284] Artikel 18/10, artikel 4.
[285] Artikel 43/2 tot en 43/4 W.IenV.

bevoegd om de rechtmatigheid aan de hand van proportionaliteit en subsidiariteit van de inzet van alle bevoegdheden te toetsen.[286] Het VCI heeft tevens de bevoegdheid om beslissingen van de BIM-commissie die voorafgaand aan de uitvoering toestemming verleent, ongeldig te verklaren.[287] Het VCI kan onderzoek uit eigen beweging starten, of op verzoek van de BIM-Commissie voor de bescherming van de persoonlijke levenssfeer of naar aanleiding van een klacht. Het toezichtsorgaan heeft toegang tot alle informatie en de betrokken inlichtingen- en veiligheidsdiensten zijn gehouden onverwijld iedere informatie te verstrekken indien het VCI hierom verzoekt.[288]

Het VCI is tevens belast met de behandeling van klachten over de rechtmatigheid van de inzet van de specifieke en uitzonderlijke bevoegdheden. De uitspraken zijn bindend en vaststelling van onrechtmatigheid kan leiden tot het staken van de inzet van de uitzonderlijke bevoegdheid en het vernietigen van de verzamelde gegevens.[289] Het VCI rapporteert elk halfjaar aan de Senaat over de klachtbehandeling. Het kan in de hoedanigheid van klachtbehandelaar eveneens voorafgaande toestemmingverleningen van de BIM-commissie overrulen.[290] Tegen de beslissing van het VCI is geen beroep mogelijk.

De ADIV is bevoegd om bulkinterceptie uit te voeren. De wet kent een regeling voor de toestemmingverlening voor de voorgenomen bulkinterceptie door de ADIV met het oog op het verzamelen van informatie over het buitenland. Deze dienst is op grond van een strafuitsluiting in het Strafwetboek bevoegd over te gaan tot interceptie van communicatie 'uitgezonden in het buitenland'.[291] Voor de activiteiten van de ADIV verleent de Minister van Landsverdediging toestemming op basis van een jaarlijks door de ADIV op te stellen lijst met instellingen en organisaties waarnaar onderzoek wordt verricht. De lijst vermeldt tevens een motivering en de toestemming geldt voor de duur van maximaal een jaar. Bewaartermijnen ter zake van in bulk geïntercepteerde internationale communicatie zijn niet in de wet vastgelegd. Zowel metadata als de

[286] Artikel 43/2, eerste lid.
[287] Wanneer het Vast Comité I de onwettigheid van de beslissingen met betrekking tot specifieke of uitzonderlijke methoden vaststelt, beveelt het de stopzetting van de betrokken methode indien deze nog steeds in uitvoering is of indien zij werd geschorst door de commissie, en beveelt het dat de gegevens die met deze methode werden verkregen niet mogen worden gebruikt en dienen te worden vernietigd. Wanneer echter het Vast Comité I van oordeel is dat de BIM-commissie ten onrechte de exploitatie van de betrokken gegevens heeft verboden, evenals deze specifieke of uitzonderlijke methode in kwestie heeft geschorst, kan het Comité het verbod en de schorsing opheffen door middel van een met redenen omklede beslissing.
[288] Artikel 45/5, eerste lid, Wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdienst.
[289] Artikel 43/6, eerste lid, eerste volzin W.IenV.
[290] Artikel 43/6, eerste lid, derde volzin W.IenV.
[291] Deze bepaling regelt een uitzondering op de strafbaarstelling van het onderscheppen van communicatie die is uitgezonden in het buitenland en luidt 'De bepalingen van § 1, 1° en 2° [van 259Bis strafwetboek], zijn niet van toepassing op [het zoeken,] het onderscheppen, het afluisteren, het kennisnemen of het opnemen door de Algemene Dienst inlichting en Veiligheid van de Krijgsmacht van elke vorm van communicatie uitgezonden in het buitenland zowel om redenen van militaire aard in het kader van de opdrachten gedefinieerd in artikel 11, § 2, 1° en 2°van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdienst als om redenen van veiligheid [Wet V.en.I] en bescherming van onze troepen en van deze van onze geallieerden tijdens opdrachten in het buitenland en van onze onderdanen die in het buitenland gevestigd zijn, […].

inhoud van communicatie kan in beginsel onbeperkt worden bewaard. De wetgeving maakt geen onderscheid naar kabelgebonden en niet-kabelgebonden interceptie. Het toezicht door het VCI gedurende de interceptie wordt uitgeoefend door middel van bezoeken aan de installaties waar de ADIV de intercepties uitvoert, en gebeurt aan de hand van een logboek dat permanent op de plaats van de interceptie door de ADIV wordt bijgehouden.[292] Het logboek is steeds toegankelijk voor het VCI. Het VCI heeft de bevoegdheid de lopende intercepties te laten stopzetten indien blijkt dat de voorwaarden waaronder ze worden uitgevoerd de wettelijke bepalingen en/of de toestemming niet respecteren.[293] Voor de BIM-commissie is in het kader van bulkinterceptie in het buitenland of met betrekking tot buitenlandse communicatie geen voorafgaand rechtmatigheidstoezicht weggelegd.

10.6. Vergelijkende observaties

Samenvattend

De onderzochte landen Duitsland, het Verenigd Koninkrijk, Frankrijk en België beschikken alle over de wettelijke bevoegdheid gegevens in bulk te intercepteren. De wijze waarop de bevoegdheden en de waarborgen in de verschillende landen zijn vastgelegd laat een divers beeld zien; over toezicht en bulkinterceptie bestaan geen geharmoniseerde regelingen. De onderzochte landen kennen anders dan Nederland traditioneel afzonderlijke inlichtingen-, veiligheids-, en soms aparte SIGINT-diensten. Landen differentiëren in het beschermingsregime in relatie tot het eigen grondgebied. Daardoor worden staatsburgers in binnen- en buitenland meer beschermd met waarborgen in de toestemmingen- en toezichtsfeer dan niet-ingezetenen en in het buitenland communicerende partijen.

Geen onderzocht land kent een afzonderlijk wettelijk toestemmingenregime voorafgaand aan de inzet van bijzondere bevoegdheden in het buitenland. In Frankrijk heeft de wetgever in 2015 getracht een dergelijk toestemmingsregeling in de CSI op te nemen, maar dat bleek niet mogelijk vanwege het ontbreken van jurisdictie buiten het eigen territorium. Een overeenkomst tussen de landen is dat indien de inzet van bevoegdheden niet op het eigen territorium plaatsvindt, de bewindspersoon/dienst die het aangaat vanuit zijn verantwoordelijk voor de goede taakuitvoering steeds de noodzaak ervan beoordeelt en toestemming verleent.

In alle onderzochte landen is de wetgeving omtrent inlichtingen- en veiligheidsdiensten in beweging, hetgeen mede wordt veroorzaakt door grotendeels publieke en politieke discussies over de bevoegdheden van de inlichtingen- en veiligheidsdiensten. Zowel

[292] Artikel 44bis, tweede lid, W.IenV.
[293] Artikel 44ter, eerste volzin W.IenV.

nationale als internationale rechtspraak, de onthullingen van de (wettelijke) werkwijzen van de diensten alsook en de aanslagen in onder meer België, Frankrijk en Engeland in de afgelopen jaren, hebben in diverse landen hebben onmiskenbaar aandacht gevestigd op de verhouding tussen de technologische ontwikkelingen en de effectiviteit van bevoegdheden en van de grondrechtelijke waarborgen. In alle onderzochte landen ondergingen wetten recentelijk, of ondergaat wetgeving thans een modernisering.

Vergelijking met Nederland

Anders dan de beschreven landen beschikt Nederland over twee diensten die beide taken hebben op het gebied van zowel inlichtingen als veiligheid. De modernisering van de Wiv 2002 vormt geen aanleiding om deze situatie te veranderen. Dit brengt met zich mee dat bijzondere bevoegdheden, zoals onderzoeksopdrachtgerichte interceptie, beide diensten toekomen en het toezicht voor beide diensten op gelijke wijze is ingericht.

Het controlesysteem op de Nederlandse inlichtingen- en veiligheidsdiensten wordt met dit wetsvoorstel aangescherpt. Met een toets voorafgaand aan de daadwerkelijke uitoefening van een bijzondere bevoegdheid door de nieuwe onafhankelijke toetsingscommissie (TIB), toezicht tijdens en achteraf van de onafhankelijke CTIVD en de mogelijkheid een klacht in te dienen bij de CTIVD die in dat geval een bindend oordeel geeft, is het stelsel van rechtsbescherming aanmerkelijk verbeterd. In lijn met de Europese jurisprudentie op dit terrein kunnen ingrijpende bevoegdheden niet worden uitgeoefend zonder voorafgaande, onafhankelijke toets. Ook met het oog op de voorgaande internationale vergelijking, mag worden gesteld dat Nederland hiermee koploper is.

Bij de modernisering van het interceptiestelsel van de Wiv 2002 heeft de regering zich goed rekenschap gegeven van interne en externe dreigingen en het feit dat vanuit Nederland zeer ernstige dreigingen voor buurlanden kunnen ontstaan. Daarenboven fungeert Nederland als internationale *hub* voor datacommunicatie. Dit brengt een bijzondere verantwoordelijkheid met zich mee. Anders dan in enkele andere landen maakt de regering geen juridisch onderscheid naar binnenlandse en buitenlandse telecommunicatie. Het kunnen verwerken van binnenlandse communicatie is noodzakelijk voor het effectief aangrijpen van binnenlandse dreigingen (met mogelijk buitenlandse gevolgen), het kunnen tegengaan van cyberdreigingen en voor het kunnen achterhalen van ongekende dreigingen. Ook is het interceptiestelsel hiermee toekomstvast; gelet op de dynamische en in voorkomend geval internationale routering van telecommunicatie en technologische ontwikkelingen zoals de *cloud,* is het onderscheid binnenland-buitenland slechts betrekkelijk. Voor onderzoeksopdrachtgerichte interceptie is de maximale bewaartermijn op drie jaar

gesteld. Wij sluiten hiermee op hoofdlijnen aan op hetgeen gebruikelijk is in de landen om ons heen. Met de plicht van de diensten via bijzondere bevoegdheden verkregen data zo spoedig mogelijk op relevantie onderzoeken en niet-relevante te vernietigen, is een extra waarborg gecreëerd, die in andere landen vaak niet bestaat.

Hoofdstuk 11 Financiële gevolgen voor het Rijk en het bedrijfsleven

Dit wetsvoorstel laat voor een groot deel de bestaande praktijk bij de diensten ongewijzigd. Ten aanzien van gewijzigde bevoegdheden wordt onderstaand uiteengezet wat de financiële gevolgen zijn voor overheid en bedrijfsleven. Ook wordt ingegaan op de effecten van de versterking van toezicht en toetsing.

In algemene zin wordt opgemerkt dat de financiële gevolgen voor het bedrijfsleven zeer beperkt zullen zijn. In samenwerking met het bedrijfsleven zijn de bedrijfseffecten nader in kaart gebracht. Hiertoe is een bedrijfseffectentoets (BET) uitgevoerd. Dit is het instrument om bij nieuwe en wijzigende regelgeving in kaart te brengen wat de gevolgen voor het bedrijfsleven kunnen zijn.

Kabelgebonden interceptie
Een belangrijk onderdeel van het wetsvoorstel is de bevoegdheid van de diensten tot onderzoeksopdrachtgerichte interceptie (artikel 48). Deze bevoegdheid heeft onder meer betrekking op telecommunicatie die via kabelgebonden netwerken verloopt. Ten behoeve van de uitvoering van deze bevoegdheid kunnen aanbieders van communicatiediensten worden verplicht medewerking te verlenen.

De vraag is of een vergoeding in redelijkheid van de kosten die een aanbieder moet maken als direct gevolg van de inzet van deze bevoegdheid een passend uitgangspunt is. In principe vergoedt de overheid niet de investeringskosten aan bedrijven aan wie de verplichting wordt opgelegd om mee te werken aan de uitvoering van een overheidstaak. In dit geval acht de regering een kostenvergoeding naar redelijkheid wel opportuun en aan de orde. Dit gegeven het feit dat onderzoeksopdrachtgerichte interceptie selectief plaatsvindt en dat deze kosten daardoor kunnen neerslaan bij slechts één of enkele aanbieders van communicatiediensten. Zonder een vergoeding naar redelijkheid zal het gelijke speelveld in deze sector worden verstoord. In de praktijk betekent dat in deze specifieke omstandigheden de kosten worden vergoed die direct samenhangen met de uitvoering van een bevoegdheid, mits het bedrijf een deugdelijke verantwoording kan overleggen. Het verantwoorden van gemaakte kosten is een administratieve last die voor rekening van het bedrijfsleven komt. Dit is evenwel een gebruikelijke en redelijke eis om voor vergoeding van kosten door de overheid in aanmerking te kunnen komen.

Op termijn moeten de effecten van deze wet en zijn uitvoering op de kosten van aanbieders worden bezien. Hierbij moet vooral worden beoordeeld of het selectieve karakter van de interceptie nog steeds geldt.

De inzet van onderzoeksopdrachtgerichte interceptie zal, wanneer daar een aanbieder van een communicatiedienst bij is betrokken, in de regel in de volgende stappen zijn te onderscheiden:

Er is een voorbereidende fase, waarin zal moeten worden vastgesteld op welke plek in de infrastructuur ontvangst van gegevens door de diensten noodzakelijk is. Dit geschiedt primair door aanbieders te bevragen op hiervoor relevante aspecten (artikel 52). Deze informatieplicht kan leiden tot personeels- en administratiekosten. Deze kosten worden vergoed.

Voorts kan er een controle nodig zijn of de op een bepaalde locatie benodigde datastroom werkelijk aanwezig is. Dit vereist medewerking van de desbetreffende aanbieder (artikel 53) en vanzelfsprekend toestemming voor interceptie als bedoeld in artikel 48 en onderzoek als bedoeld in artikel 49. De kosten die de aanbieder in dit kader maakt, zoals de inzet van ondersteunende mankracht en eventuele technische voorzieningen, worden vergoed.

Wanneer interceptie gedurende langere tijd aan de orde is, zullen de hiermee gepaard gaande kosten eveneens worden vergoed. Dit kan gaan om investeringskosten om duplicatie van een datastroom gedurende langere tijd te kunnen faciliteren. Direct verband houdende exploitatiekosten, zoals voor stroomvoorziening en koeling van door de diensten geplaatste apparatuur, worden eveneens vergoed.

Op het moment dat interceptie niet langer aan de orde is, zal op enig moment ontmanteling van de locatie aan de orde zijn. Ook de kosten die hiermee zijn gemoeid, worden vergoed.

Om de redelijkheid van de vergoeding van een daarvoor in aanmerking komende aanbieder van een communicatiedienst te waarborgen, zal de overheid de kosten die de betreffende aanbieder opgeeft toetsen. In het wetsvoorstel is opgenomen (artikel 53) dat bij ministeriële regeling regels worden gesteld met betrekking tot de vaststelling en de vergoeding van de kosten. De komende periode zal deze regeling in overleg met daarvoor relevante bedrijven in de telecommunicatiebranche worden opgesteld.

Overige bevoegdheden in relatie tot telecommunicatie

Met de introductie van het begrip ‘aanbieder van een communicatiedienst’ (artikel 46) is de kring van aanbieders die ook gebruikersgegevens en verkeersgegevens moeten kunnen verstrekken en medewerking moeten verlenen aan gerichte interceptie van communicatie uitgebreid. De kring van aanbieders bestaat in de eerste plaats uit de

traditionele aanbieders van openbare telecommunicatienetwerken en openbare telecommunicatiediensten conform de algemene bepalingen van de Telecommunicatiewet (Tw). Voor deze aanbieders geldt onverminderd het systeem van kostenvergoedingen zoals neergelegd in artikel 13.6 Tw.

Ook andersoortige aanbieders van communicatiediensten verwerken telecommunicatie die noodzakelijk kan zijn voor de goede taakuitvoering van de diensten. Voorbeelden hiervan zijn aanbieders van hosting- en clouddiensten. Ook deze aanbieders moeten desgevraagd bij hen aanwezige gebruikersgegevens en verkeersgegevens kunnen verstrekken. De gemaakte administratie- en personeelskosten rechtstreeks voortvloeiend uit het voldoen aan deze plicht, worden in redelijkheid door het Rijk vergoed. Wat betreft de plicht tot het verlenen van medewerking aan de gerichte interceptie van communicatie, zoals bedoeld in artikel 47, eerste lid, van het wetsvoorstel, geldt dat het passend wordt geacht de kosten die een dergelijke aanbieder in dat kader maakt naar redelijkheid te vergoeden. Artikel 53, zevende lid, van het wetsvoorstel voorziet hier in, aangezien het voor deze groep aanbieders - anders dan voor openbare aanbieders - niet redelijk is te verwachten dat vooraf reeds organisatorische en technische maatregelen worden getroffen om interceptie te kunnen faciliteren.

Een nieuwe bevoegdheid in het wetsvoorstel houdt verband met het opvragen van opgeslagen telecommunicatie. Kort samengevat biedt artikel 54 de diensten de mogelijkheid zich te wenden tot aanbieders, bijvoorbeeld een bedrijf dat bestandsopslag en -uitwisseling in de cloud verzorgt, met de opdracht de relevante door hen opgeslagen gegevens te verstrekken. De benaderde dienstverlener is verplicht aan deze opdracht te voldoen. Dit kan leiden tot personeels- en administratiekosten. Deze worden, gelet op het feit dat artikel 13.6, tweede en derde lid, van de Telecommunicatiewet van overeenkomstige toepassing is verklaard, vergoed.

Samengevat bieden artikel 45 en artikel 57 de diensten de bevoegdheid zich te wenden tot degenen die kennis dragen van de wijze van encryptie van gesprekken, telecommunicatie of gegevensoverdracht, met de opdracht alle noodzakelijke medewerking te verlenen voor decryptie. Degene aan wie deze opdracht wordt gericht is verplicht daaraan te voldoen. 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 daarmee gepaard gaande kosten voor betrokkene is geen vergoedingsregeling getroffen. Met dit wetsvoorstel worden eventuele kosten die rechtstreeks voortvloeien uit het voldoen aan deze plicht in redelijkheid door het Rijk vergoed.

<u>Kosten binnen de overheid</u>

Uitvoering toezicht en toetsing

Er zijn meerkosten verbonden aan de nieuw in te stellen toetsingscommissie inzet bevoegdheden (TIB) en de versterking van de CTIVD, met name gelet op de klachtbehandeling. Het betreft voornamelijk personele kosten, begroot op 1 M€. De benodigde middelen voor deze intensivering zullen te zijner tijd worden toegevoegd in de Rijksbegroting hoofdstuk III, Algemene Zaken.

Kosten bij AIVD en MIVD

Met de uitvoering van kabelgebonden interceptie onder artikel 48 van dit wetsvoorstel zijn ook aan de zijde van de diensten kosten gemoeid. Het gaat om de uitgaven voor de technische interceptie, de versterking van de personele capaciteit en aanpassing van werkprocessen en informatiesystemen bij de diensten. Bij de ontwikkeling van technische systemen is transparantie en controleerbaarheid, onder andere met het oog op toezicht door de CTIVD, een uitgangspunt. De onderstaande geraamde bedragen (in miljoen €) berusten op technisch onderzoek en ervaringsgegevens en zijn inclusief de voorgaand geschetste vergoedingen die samenhangen met de toepassing van onderzoeksopdrachtgerichte interceptie en de overige bevoegdheden bij aanbieders van een communicatiedienst.

2017	2018	2019	2020	2021
20	20	20	20	20

Overleg met relevante aanbieders in de telecomsector is nodig 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 sprake van schaalbaarheid in omvang en tijd. De keuzes die hierbij worden gemaakt, hebben vanzelfsprekend financiële gevolgen. De regering beschouwt de bovenstaande bedragen als kaderstellend voor implementatie en toepassing van de uitoefening van de bevoegdheid (inclusief de vergoeding van de kosten die door het bedrijfsleven worden gemaakt). De betrokken departementen zullen de mate waarin van deze bevoegdheid gebruik wordt gemaakt, de opbrengsten ervan voor de taakuitoefening van de diensten en de hiermee samenhangende kosten, jaarlijks evalueren en betrekken bij het bepalen van het ambitieniveau.

Hoofdstuk 12 Consultatie, privacy impact assessment en notificatie

12.1 Algemeen

Een concept van het wetsvoorstel is in de maanden juli en augustus 2015 aan internetconsultatie onderworpen (in het onderstaande aangeduid als concept-wetsvoorstel). Dat heeft tot meer dan 1.100 reacties geleid van burgers, bedrijven en organisaties. Van deze 1.100 reacties heeft ongeveer de helft van de respondenten ervoor gekozen hun reactie niet openbaar te maken; de openbare reacties zijn te raadplegen op www.internetconsultatie.nl. In paragraaf 12.2 wordt op de hoofdlijnen van de ontvangen reacties ingegaan – zoveel mogelijk gerangschikt naar thema – en de wijze waarop daaraan in het wetvoorstel en de memorie van toelichting gevolg is gegeven. Omtrent het concept-wetsvoorstel is voorts aan twee organisaties, te weten de Nationale ombudsman (No) en de Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten, (CTIVD) een reactie gevraagd. De reden daarvoor is, dat de in het wetsvoorstel voorgestelde regeling inzake toezicht en klachtbehandeling directe gevolgen voor de bevoegdheid onderscheidenlijk de taken en organisatie van de betreffende organisaties heeft. Beide organisaties hebben een reactie uitgebracht; daarop zal eveneens in paragraaf 12.2 worden ingegaan. Er is geen advies gevraagd aan de Autoriteit Persoonsgegevens (AP) , aangezien het AP geen bevoegdheid toekomt waar het gaat om de verwerking van persoonsgegevens door inlichtingen- en veiligheidsdiensten; die rol komt immers (uitsluitend) toe aan de CTIVD[294]. Tot slot is met betrekking tot het concept-wetsvoorstel een Privacy Impact Assessment (PIA) opgesteld. Over het voornemen tot het doen uitvoeren van een PIA is de Tweede Kamer bij brief van 17 maart 2015 door de ministers van BZK en Defensie nader geïnformeerd.[295] In paragraaf 12.3 wordt op de PIA, die door het PI.lab (Privacy & Identity Lab) is uitgevoerd, alsmede de daaraan verbonden conclusies ingegaan. Hoewel diverse opmerkingen en bevindingen naar aanleiding van de PIA ook in het kader van de internetconsultatie naar voren zijn gebracht, worden deze separaat daarvan besproken. Het rapport van het PI.lab is bij brief van 3 mei 2016 door de minister van BZK, mede namens de minister van Defensie, aan de Tweede Kamer aangeboden (kamerstukken II, 2015/16, 33 820, nr. 7).

12.2. Consultatie

12.2.1 Inleiding

[294] Op grond van artikel 2, tweede lid, onder b is de Wet bescherming persoonsgegevens niet van toepassing verklaard op verwerking van persoonsgegevens door of ten behoeve van de inlichtingen- en veiligheidsdiensten.
[295] Kamerstukken II 2014/15, 33 820, nr. 5.

In het kader van de consultatieronde zijn zoals hiervoor aangegeven meer dan 1100 reacties ontvangen. Naast de reacties van vele burgers, zijn reacties ontvangen van diverse organisaties en bedrijven. Het gaat daarbij onder meer om het College voor de Rechten van de Mens (CRvdM), het Nederlands Juristencomité voor de Mensenrechten (NJCM), het Instituut voor Informatierecht (IViR), Bits of Freedom (BoF), Vereniging voor Media- en Communicatierecht (Studiecommissie Journalistieke Bronbescherming)(VMC), Free Press Unlimited, Nederlandse Orde van Advocaten (NOvA), Amnesty International (AI), Internet Society Nederland (ISOC NL), Privacy International (PI), Nederland ICT, Surf, Stichting DNIL, Privacy Barometer, KPN, Tele2, T-Mobile, Vodafone, VNO-NCW, Microsoft, Arthur's Legal, Google en BCPA.

Het gros van de reacties die van burgers zijn ontvangen, lijkt – vanwege de inhoud – gegenereerd te zijn onder gebruikmaking van de door BoF ontworpen "internetconsultatie tool Wet op de inlichtingen- en veiligheidsdiensten"[296] , die deze digitale burgerrechtenorganisatie op 12 augustus 2015 aan het publiek ter beschikking heeft gesteld. De hoofdpunten van kritiek in de desbetreffende reacties zien vrijwel allemaal op drie onderwerpen: groot sleepnet, samenwerking met buitenlandse geheime diensten en goed toezicht. Deze kritiekpunten komen voor een groot deel overeen met vergelijkbare kritiek uit andere ontvangen reacties en zullen in het onderstaande worden meegenomen.

De meeste reacties zien grotendeels op een beperkt aantal onderdelen van het wetsvoorstel. Het gaat dan in het bijzonder om (1) de in het wetsvoorstel voorgestelde aanpassing van het interceptiestelsel, in het bijzonder de voorgenomen uitbreiding van de bevoegdheid tot het onderzoeksopdrachtgericht intercepteren van telecommunicatie tot het kabelgebonden domein (in de reacties ook wel als bulkinterceptie aangeduid) en de effecten daarvan voor de markt en bedrijven, (2) het voorziene toezichts- en klachtstelsel, waarbij met name ook aandacht is gevraagd voor de toestemmingverlening met betrekking tot de meer ingrijpende bijzondere bevoegdheden, (3) het binnendringen in geautomatiseerde werken, (4) de medewerkingsplicht bij het ontsleutelen van telecommunicatie en gegevens en (5) de samenwerking met buitenlandse diensten. Een beperkt aantal respondenten, waaronder met name de CTIVD, is in haar reactie ook ingegaan op diverse andere onderdelen van het wetsvoorstel (en de memorie van toelichting) en heeft daarbij suggesties tot aanpassing gedaan. Onder het kopje capita selecta zullen aansluitend nog de opmerkingen met betrekking tot enkele andere opgebrachte onderwerpen aan de orde worden gesteld.

[296] wiv.bof.nl

Gelet op de grote hoeveelheid aan reacties is ervoor gekozen om deze zoveel mogelijk samen te nemen en geparafraseerd weer te geven.

12.2.2 Het nieuwe interceptiestelsel

De in het concept-wetsvoorstel opgenomen regeling voor een nieuw interceptiestelsel, in het bijzonder de regeling die het mogelijk maakt dat voortaan niet alleen niet-kabelgebonden telecommunicatie (etherverkeer) onderzoeksopdrachtgericht kan worden geïntercepteerd[297] maar ook kabelgebonden telecommunicatie, alsmede de daarmee samenhangende informatie- en medewerkingsplichten[298], stuit op kritiek van veel respondenten (naast vele burgers, onder meer van KPN, Tele2, T-Mobile, Privacy First, Privacy Barometer, Nederland ICT, NJCM, DNIL, Amnesty International, BoF). Deze kritiek richt zich – mede afhankelijk van de positie van de respondent – op diverse aspecten die aan het voorstel zijn verbonden. Zo wordt erop gewezen dat een toereikende onderbouwing voor het voorstel ontbreekt, waar het gaat om *nut en noodzaak* van de voorgestelde bevoegdheidsuitbreiding alsmede de *effectiviteit* en de *proportionaliteit* ervan. Onder het mom van *techniekonafhankelijkheid* zou, aldus diverse respondenten, een wezenlijke uitbreiding van de bevoegdheden van de inlichtingen- en veiligheidsdiensten worden geïntroduceerd. De nieuwe bevoegdheid zou het mogelijk maken alle burgers, ook als ze onverdacht zijn, af te luisteren. Het voorstel kent volgens diverse respondenten nog veel onduidelijkheden en onvoldoende waarborgen; dat komt tot uitdrukking in diverse aspecten, zoals de reikwijdte van de medewerkingsverplichting (op wie is de regeling van toepassing?), het begrip aanbieder van communicatiediensten), de toestemmingverlening voor de uitoefening van de bevoegdheid (niet onafhankelijk), de vaagheid van het begrip 'doelgerichtheid' en de doorverstrekking aan buitenlandse collegadiensten. Een veel terugkomende opmerking betreft de bewaartermijnen die in het nieuwe stelsel zijn voorzien; de termijnen worden te lang geacht, zijn onvoldoende gemotiveerd, en kunnen mogelijk de toets van het EVRM niet doorstaan. Een ander belangrijk punt van kritiek betreft de in het wetsvoorstel neergelegde stelsel van kostenverdeling tussen overheid en bedrijfsleven, waarbij – in het bijzonder waar het gaat om de kosten verbonden aan de uitvoering van een verleende toestemming tot onderzoeksopdrachtgerichte interceptie – is aangesloten bij het model van kostenverdeling, zoals neergelegd in artikel 13.6 van de Telecommunicatiewet (Tw); de desbetreffende kosten zouden echter geheel voor rekening van de overheid moeten komen. Volgens de respondenten is de gekozen kostenverdeling disproportioneel. Bovendien is volgens hen het geheel niet duidelijk wat de omvang is van de te verwachten kosten. Ook wordt door een enkeling (KPN) gepleit

[297] Artikel 27, eerste lid, Wiv 2002 geeft de AIVD en MIVD de bevoegdheid om ongericht niet-kabelgebonden telecommunicatie te intercepteren.
[298] De artikelen 33 e.v. van het in consultatie gegeven concept-wetsvoorstel.

om de medewerkingsverplichtingen in de Tw te regelen, mede om daarmee naleving van het EU-recht te verzekeren; idem waar het gaat om de gehanteerde definities. In algemene zin wordt door verschillende respondenten aangegeven dat met het wetsvoorstel het imago van Nederland als vestigingsplaats voor innovatieve bedrijven in de ICT-sector wordt geschaad. Een onderzoek naar de gevolgen van het voorstel voor het vestigingsklimaat en andere daarmee verbonden economische gevolgen ontbreekt.

In de internetconsultatie is door veel respondenten aangegeven dat *nut en noodzaak* van de voorgestelde uitbreiding van het interceptiestelsel alsmede de *effectiviteit* en de *proportionaliteit* ervan niet dan wel onvoldoende is aangetoond. Er zijn voldoende argumenten die het voorstel kunnen dragen, maar die waren– gelet op de kritische reacties - nog niet adequaat en toereikend verwoord. De toelichting op het nieuwe interceptiestelsel is naar aanleiding hiervan aangevuld; verwezen wordt naar paragraaf 3.3.4.4.7.4 van de toelichting. De kritiek dat de nieuwe bevoegdheid (in het wetsvoorstel aangeduid als onderzoeksopdrachtgerichte interceptie) neer zou komen op een sleepnetbevoegdheid wordt afgewezen. Erkend wordt dat met de uitoefening van de bevoegdheid – of dat nu in het niet-kabelgebonden domein (wat nu reeds plaatsvindt op basis van artikel 27 Wiv 2002) of in het kabelgebonden domein (nieuw) plaatsvindt – gegevens worden geïntercepteerd van een grote hoeveelheid personen en instanties; dat is inherent aan onderzoeksopdrachtgerichte interceptie van grote hoeveelheden data. Bij gerichte interceptie is de interceptie gericht op een specifieke persoon of organisatie, doorgaans het target. Het komt er dan ook op aan dat zowel bij het verzoek om toestemming tot verwerving als bij de verdere verwerking van de geïntercepteerde gegevens in toereikende waarborgen wordt voorzien. Allereerst om te borgen dat er niet meer gegevens worden geïntercepteerd dan strikt nodig is voor het desbetreffende onderzoek en het daarmee beoogde doel. Voorts dat na de interceptie de relevantie van de geïntercepteerde gegevens zo snel mogelijk wordt vastgesteld (inspanningsverplichting) en niet-relevante gegevens zo spoedig mogelijk worden vernietigd. Dit laatste is – mede naar aanleiding van de PIA Wiv – in een nieuwe bepaling, te weten artikel 27, in het wetsvoorstel neergelegd. In die regeling is tevens als hoofdregel bepaald dat gegevens die na een periode van een jaar niet op hun relevantie zijn onderzocht, dienen te worden vernietigd. Daarmee is de maximale bewaartermijn (zij het met een eenmalige verlengingsmogelijkheid met zes maanden) vastgesteld. Voor de gegevens die in het kader van de onderzoeksopdrachtgerichte interceptie zijn verworven is de genoemde periode op drie jaar gesteld. De waarborgen in het wettelijk stelsel – overigens breder dan alleen waar het gaat om de voorgestelde nieuwe interceptiebevoegdheid – zijn voorts aan de voorkant versterkt door de introductie van een onafhankelijke toets op de door de minister verleende toestemming. In paragraaf 3.2.2 van het wetsvoorstel wordt voorzien in de instelling van een

onafhankelijke Toetsingscommissie inzet bevoegdheden (TIB), die een rechtmatigheidsoordeel moet geven over de door de minister verleende toestemming. In afwachting van dat oordeel mag de bevoegdheid, in casu de interceptiebevoegdheid, nog niet worden uitgeoefend; indien de TIB van oordeel is dat de toestemming niet rechtmatig is verleend, vervalt de toestemming van rechtswege. In paragraaf 3.3.3 wordt deze toets nader toegelicht; zie ook paragraaf 12.2.3 hieronder.

Een ander punt van kritiek betreft de reikwijdte van de medewerkingsverplichting, met name waar het gaat om de categorie aanbieders van communicatiediensten. In het wetsvoorstel zoals dat ter consultatie is aangeboden, is er voor gekozen om de medewerkingsplicht, waar het gaat om de diverse bevoegdheden die worden geschaard onder de noemer "onderzoek van communicatie", te doen uitstrekken tot de categorie aanbieders van communicatiediensten en daarin niet te differentiëren waar het gaat om de soort bevoegdheid. Met deze definitie is aangesloten bij de definitie uit artikel 126la Wetboek van Strafvordering (Sv). Ook in Sv is voor deze categorie gekozen waar het gaat om de interceptiebevoegdheid (artikel 126m Sv) alsmede andere bevoegdheden in de sfeer van onderzoek van communicatie. In onder meer de reactie van Tele2 wordt erop gewezen dat de categorie aanbieders van communicatiediensten een zeer grote groep van ongeveer 360.000 instanties kan betreffen. Dit is voor het antwoord op de vraag of het noodzakelijk is om de medewerkingsplicht tot de hier bedoelde categorie te doen uitstrekken niet relevant. In paragraaf 3.3.4.4.7.2 van deze toelichting is ingegaan op het begrip aanbieders van communicatiediensten en nader uiteengezet waarom daarvoor is gekozen. Waar het gaat om de bevoegdheid van de diensten tot onderzoeksopdrachtgerichte interceptie zal in de praktijk naar verwachting overigens slechts een beperkt aantal categorieën van aanbieders, met name aanbieders van communicatienetwerken, benaderd worden voor medewerking. Met het oog op de toekomstvastheid van de regeling is ervoor gekozen om niet op voorhand enige beperking aan te brengen. De bedrijfseffecten van de voorgestelde onderzoeksopdrachtgerichte interceptiebevoegdheid worden in overleg met het bedrijfsleven de komende periode in kaart gebracht; zie hoofdstuk 11 van deze toelichting.

In diverse reacties[299] is de regeling inzake de kostenverdeling, zoals die in het in consultatie gegeven wetsvoorstel was opgenomen, stevig bekritiseerd. Daarbij was de regeling van artikel 13.6 Tw van overeenkomstige toepassing verklaard op die aanbieders van communicatiediensten niet zijnde aanbieders van openbare telecommunicatienetwerken en –diensten als bedoeld in de Tw, zowel waar het gaat om de gerichte interceptie als de onderzoeksopdrachtgerichte interceptie. Dat zou met zich

[299] En ook in de PIA Wiv.

mee brengen dat zij zelf de investerings-, exploitatie- en onderhoudskosten zouden moeten dragen voor de technische voorzieningen om aan een taplast te kunnen voldoen. De geuite kritiek heeft ertoe geleid dat dit onderdeel van het wetsvoorstel is heroverwogen en besloten is de desbetreffende kosten – waar het gaat om genoemde categorie van aanbieders van communicatiediensten - alsnog te naar redelijkheid vergoeden. Afwijking van de Tw, in casu de gerichte tap bij openbare aanbieders, is aan de orde gelet op de veel kleinschaliger toepassing, het bijzondere en complexe karakter van deze bevoegdheid die enkel de inlichtingen- en veiligheidsdiensten toekomt en aangezien op voorhand geen zekerheid valt te geven over de vraag tot welke aanbieders de diensten zich zullen wenden en over de kosten die met interceptie zijn gemoeid. Dit zal per geval afhangen van het doel waarvoor de bevoegdheid zal worden ingezet en van de specifieke omstandigheden waaronder de interceptie moet worden uitgevoerd. Artikel 53, zevende lid, van het wetsvoorstel voorziet hier in, aangezien het voor deze groep aanbieders - anders dan voor openbare aanbieders - niet redelijk is te verwachten dat vooraf reeds organisatorische en technische maatregelen worden getroffen om interceptie te kunnen faciliteren. Voor de aanbieders van openbare telecommunicatienetwerken en -diensten verandert in geval van gerichte interceptie niets. Voor hen blijft artikel 13.6 Tw van toepassing. Bij onderzoeksopdrachtgerichte interceptie worden de investerings-, exploitatie- en onderhoudskosten echter wel naar redelijkheid vergoed. In de praktijk komt dit erop neer dat alle gemaakte kosten voor volledige vergoeding in aanmerking komen, mits kan worden aangetoond dat de kosten die men heeft gemaakt in relatie tot de noodzakelijk te treffen maatregelen in een redelijke verhouding staan en niet als overmatig kunnen worden aangemerkt. De aanbieder kan worden gevraagd dit te onderbouwen. Bij ministeriële regeling zullen nadere regels worden gesteld met betrekking tot de vaststelling en de vergoeding van de kosten.

12.2.3 Het toezichts- en klachtstelsel

Het in het concept-wetsvoorstel neergelegde toezichtstelsel, waarin uitwerking is gegeven aan het kabinetsstandpunt naar aanleiding van de voorstellen van de Commissie Dessens en zoals dat ter internetconsultatie was voorgelegd, stuitte bij diverse respondenten (onder meer Nationale ombudsman, CTIVD, diverse bedrijven in de ICT-sector, IViR, CRvdM, NJCM, Privacy First, Privacy Barometer, BoF) op kritiek. Daarin is gekozen voor handhaving van het toestemmingsvereiste bij de minister, zij het aangevuld met een heroverwegingsplicht ingeval de CTIVD tot het oordeel komt dat een verleende toestemming onrechtmatig is, met een follow up (indien aan de orde) richting de Commissie voor de Inlichtingen- en Veiligheidsdiensten (CIVD) van de Tweede Kamer. Tevens is voorzien in de positionering van de CTIVD als zelfstandige

klachtinstantie die bindende oordelen kan geven. In verband met het voorkomen van ongewenst geachte interferentie (vooringenomenheid) bij de uitoefening van de drie aan de CTIVD opgedragen (hoofd)taken, te weten rechtmatigheidstoezicht achteraf enerzijds en klachtbehandeling alsmede het onderzoeken van vermoedens van misstanden anderzijds, is voorzien in organisatorische en personele maatregelen die dit adequaat moeten borgen. Daarnaast is ervoor gekozen om de bevoegdheid van de Nationale ombudsman om klachten betreffende de inlichtingen- en veiligheidsdiensten te behandelen, te schrappen. Bij de vormgeving van dit stelsel is in het bijzonder aandacht besteed aan het stelsel dat in het Verenigd Koninkrijk geldt, waarbij de toestemming voor de uitoefening van bevoegdheden ook in handen is gelegd van de verantwoordelijke minister en is voorzien in onafhankelijke klachtbehandeling door het IPT die tevens bindende oordelen kan geven; dit stelsel is in de zaak Kennedy tegen Verenigd Koninkrijk door het EHRM in overeenstemming met het EVRM geacht.

In de vele reacties die op het concept-wetsvoorstel zijn uitgebracht, zijn diverse bezwaren tegen het daarin neergelegde en hiervoor geschetste toezichts- en klachtstelsel geuit. Deze zien op verschillende aspecten. Allereerst in meer algemene zin de vraag of met het voorgestane stelsel wel aan de eisen van het EVRM wordt voldaan. Sommige respondenten vinden dat sprake is van een minimale invulling (ondergrens EVRM), anderen zijn van oordeel dat Nederland met het stelsel gelet op de jurisprudentiële ontwikkeling een groot risico loopt dat het stelsel op korte termijn niet meer voldoet en weer anderen zijn van oordeel dat het stelsel niet aan de eisen van het EVRM voldoet. Een van de elementen waar veel aandacht aan wordt besteed in de ontvangen reacties is, met name in relatie tot het voorgestelde interceptiestelsel, de verlening van toestemming voorafgaande aan de uitoefening van die bevoegdheid (ex ante toets). In het concept-wetsvoorstel is die in handen gelegd van de voor de diensten verantwoordelijke minister, met dien verstande dat – wanneer het gehele scala aan bijzondere bevoegdheden wordt bezien – de toestemmingverlening met betrekking tot enkele andere bijzondere bevoegdheden ten opzichte van de huidige situatie naar een hoger niveau, te weten de minister persoonlijk is getild. Diverse respondenten zijn van oordeel dat de ex ante toets niet in handen van de minister zou moeten liggen, maar bij een onafhankelijk instantie, zoals bijvoorbeeld een rechter. Indien er geen ex ante toets wordt voorzien dan zou in ieder geval een bindend ex post toets door een onafhankelijke instantie moeten plaatsvinden; een enkele instantie is zelfs van oordeel dat er zowel in een bindend ex ante als een bindend ex post toezicht moet worden voorzien. De CTIVD pleit er voor om alsnog uitvoering te geven aan het voorstel van de Commissie Dessens, namelijk door de CTIVD te belasten met een (onmiddellijk) bindend rechtmatigheidsoordeel achteraf; de Nationale ombudsman is dezelfde mening toegedaan. Ook zou volgens een enkele respondent de doorgifte van persoonsgegevens

aan een buitenlandse collegadienst aan een rechterlijke toets (ex ante) moeten worden onderworpen.

In enkele reacties is ook stilgestaan bij de voorgestelde klachtregeling. De Nationale ombudsman heeft ernstig bezwaar tegen het onderbrengen van toezicht en klachtbehandeling bij één en dezelfde instantie, in casu de CTIVD. Bij klachtbehandeling zijn onafhankelijkheid en onpartijdigheid essentieel; een klacht over de handelwijze of bejegening door een dienst impliceert immers ook het toezicht daarop. Hij pleit ervoor om de klachtbehandeling onder te brengen bij een evident onafhankelijk instituut, zoals de No. De CTIVD ziet duidelijk meerwaarde in het onderbrengen van klachtbehandeling en toezicht bij hetzelfde orgaan, maar dan zonder functionele, personele en organisatorische scheiding, zoals in het concept-wetsvoorstel wordt voorzien. Die scheiding creëert naar het oordeel van de CTIVD in feite twee CTIVD's, waarbij vervolgens de vraag rijst of het in dat geval niet beter zou zijn de klachtbehandelingsfunctie bij een andere instantie onder te brengen. De CTIVD meent dat dit op een zodanig wijze is op te lossen, namelijk door inschakeling van een plaatsvervangend lid die het onderzoek naar de klacht doet ingeval over dezelfde kwestie al eerder een rechtmatigheidsoordeel is uitgesproken, zij het dat de besluitvorming ter zake van de klacht wel is voorbehouden aan de CTIVD; hiermee zou voldoende tegemoet gekomen kunnen worden aan het belang van publiek vertrouwen in de onbevooroordeelde afhandeling van klachten.

De ontvangen reacties op dit onderdeel van het concept-wetsvoorstel hebben ertoe geleid dat het oorspronkelijk voorstel is heroverwogen. Het wordt van groot belang geacht dat het wetsvoorstel (ook) op dit onderdeel EVRM-proof is, niet alleen nu maar zeker ook voor de toekomst. Deze heroverweging heeft geleid tot het schrappen van de eerder voorgestelde heroverwegingsplicht van de minister ingeval de CTIVD in het kader van haar rechtmatigheidstoezicht tot het (niet bindende) oordeel zou komen dat een door de minister verleende toestemming voor de uitoefening van een bijzondere bevoegdheid onrechtmatig zou zijn.[300] Deze heroverwegingsplicht is vervangen door een bindende toets, die plaatsvindt *na* het verlenen van de toestemming voor de uitoefening van een bijzondere bevoegdheid door een minister, maar *voorafgaand* aan de feitelijke uitvoering van de verleende toestemming. Deze toets wordt in handen gelegd van een nieuw in te stellen commissie, de TIB. Het oordeel van de TIB is bindend. Dat betekent dat indien de TIB van oordeel is dat de verleende toestemming onrechtmatig is, deze van rechtswege komt te vervallen. Er is voor gekozen deze toets niet te beleggen bij de CTIVD, aangezien dat tot een zodanige cumulatie van taken – toets, toezicht en klachtbehandeling - bij één instantie zou leiden dat daarmee – meer dan volgens

[300] Zoals vervat in artikel 102 van het in consultatie gegeven concept-wetsvoorstel.

sommige instanties, zoals de Nationale ombudsman, in het consultatievoorstel al het geval was – vraagtekens gezet zouden kunnen worden bij de onbevooroordeeldheid van de CTIVD bij de uitoefening van deze functies. De plaatsing onder één dak (van de CTIVD) zou, ondanks het aanbrengen van functionele, personele en organisatorische scheiding ("Chinese muren"), bij de buitenwereld toch teveel het beeld kunnen oproepen van de slager die zijn eigen vlees keurt. Dat is voor het aanzien van het instituut CTIVD niet goed. We hebben goede notie genomen van de bezwaren van de CTIVD tegen de voorgestelde regeling in het wetsvoorstel en van het alternatief om de klachtbehandeling in handen te leggen van een plaatsvervangend lid ingeval over dezelfde kwestie reeds een rechtmatigheidsoordeel is gegeven. Dit voorstel wordt afgewezen, omdat dit teveel afbreuk doet aan de eis van onbevooroordeeldheid die wij menen te moeten stellen aan de uitoefening van de twee aan de CTIVD opgedragen taken. Zeker het element in het voorstel van de CTIVD dat het uiteindelijke oordeel over de klacht aan de CTIVD moet worden voorbehouden, leidt juist tot een situatie die moet worden voorkomen: namelijk dat de instantie die eerst (als commissie) een rechtmatigheidsoordeel over een kwestie heeft uitgesproken later in een klachtprocedure over diezelfde kwestie, waarbij ook het oordeel in het rechtmatigheidstoezicht moet kunnen worden betrokken, (als commissie) oordeelt. Dan is van onafhankelijkheid geen sprake meer. Aangezien eraan gehecht wordt dat de bindende klachtbehandeling, zoals in het wetsvoorstel is voorgesteld, wel bij de CTIVD blijft berusten – mede gelet op de expertise die zij op dat vlak heeft – en het onderbrengen van deze functie gelet op het bindende karakter van de daarbij uit te spreken oordelen bij een instantie als de Nationale ombudsman niet aangewezen wordt geacht, is er dan ook voor gekozen de bindende toets bij een nieuw in te stellen instantie te beleggen. In paragraaf 3.3.3 van deze toelichting wordt de instelling, taakstelling en werkwijze van de TIB nader toegelicht. Met de voorgestelde versterking van het toezichtsregime in brede zin wordt een toekomstvast en EVRM-proof stelsel gecreëerd. Hiermee wordt tevens voldaan aan het merendeel van de "Ten standards for oversight and transparency of national intelligence services" zoals opgesteld door het IViR. In hoofdstuk 9, waar ingegaan wordt op de grond- en mensenrechtelijke aspecten van onderhavig wetsvoorstel, wordt daar nog nader op ingegaan.

12.2.4 Het binnendringen in geautomatiseerde werken

In het concept-wetsvoorstel is de bestaande bijzondere bevoegdheid tot het binnendringen in geautomatiseerde werken in diverse opzichten gewijzigd. Niet alleen is het toestemmingsniveau bij de minister belegd, maar ook de formulering van de bevoegdheid is aangepast. Zo zijn de mogelijkheid tot het verkennen van geautomatiseerde werken, de mogelijkheid om via een geautomatiseerd werk van een derde binnen te dringen in een geautomatiseerd werk van een target alsmede de

mogelijkheid om ter ondersteuning van de uitoefening van enkele andere bijzondere bevoegdheden in het geautomatiseerd werk van een target technische voorzieningen aan te brengen, nu expliciet beschreven in de wet. Tot slot is voorzien in een bewaar- c.q. vernietigingstermijn met betrekking tot gegevens die met de uitoefening van de bevoegdheid zijn verworven.

De voorgestelde regeling heeft diverse (kritische) reacties opgeleverd (van o.a. BoF, CTIVD, KPN, Privacy First, DHPA, MKB NL, Amnesty International). De voorziene bevoegdheid wordt over het algemeen als een zeer vergaande en diep inbreukmakende bevoegdheid op de privacy van de burgers gezien. Het binnendringen in een geautomatiseerd werk is volgens de respondenten nu een veel grotere inbreuk dan in 1998 bij de indiening van het voorstel voor de huidige Wiv 2002 werd voorzien. Er zou in de toelichting aandacht geschonken moeten worden aan de reikwijdte en de wenselijkheid van deze bevoegdheid. Respondenten wijzen erop dat bijvoorbeeld niet wordt ingegaan op ontwikkelingen als de Internet of Things en de betekenis van de bevoegdheid daarvoor. De (uitoefening van de) bevoegdheid brengt volgens hen vele risico's met zich mee; niet alleen voor de betrokkene waarop de bevoegdheid wordt ingezet (zeker ingeval de inzet plaatsvindt op een derde, niet zijnde het target), maar ook voor de integriteit en betrouwbaarheid van het internet en de daarop aangesloten ICT-systemen. Het gebruik van *malware* en het exploiteren van in geautomatiseerde werken onderkende zwakheden kan volgens hen vergaande gevolgen hebben, die niet op voorhand zijn te voorzien en te controleren. Volgens de respondenten zou ook een regeling moeten komen voor het verkrijgen, gebruiken en delen van zwakheden in ICT-systemen door de diensten. De overheid zou onderkende zwakheden volgens hen moeten melden aan het Nationaal Cyber Security Centrum (NCSC). Zeker nu het gehele nationale beleid en Europese beleid is gericht om digitale infrastructuren te beveiligen en te beschermen tegen ingrijpen van buiten en er in dat kader steeds verdergaande continuïteits- en beveiligingsverplichtingen aan telecomaanbieders wordt opgelegd, staat het toekennen van een bevoegdheid aan de inlichtingen- en veiligheidsdiensten om op die netwerken binnen te mogen dringen daar haaks op (KPN). Hoe gaat men om met de paradoxale situatie dat enerzijds een dienst moet kunnen binnendringen in geautomatiseerd werk en daarbij belang heeft dat kwetsbaarheden blijven bestaan en anderzijds een wettelijke verplichting voor bedrijven bestaat om alle maatregelen te treffen om hun netwerken te beveiligen inclusief een meldingsplicht? Bij het verkennen van en binnendringen van geautomatiseerde werken, zouden de netwerken waarop die geautomatiseerde werken zijn aangesloten expliciet dienen te worden uitgezonderd (KPN). BoF stelt dat het binnendringen van een geautomatiseerd werk van een target door tussenkomst van het geautomatiseerde werk van een derde zeer risicovol is. BoF geeft aan dat deze regeling voor een derde niet voorzienbaar is (onder meer wie als

derde wordt aangemerkt) en niet proportioneel; bovendien is deze mogelijkheid met niet meer waarborgen omgeven dan bij toepassing van de bevoegdheid op een target. Hoe wordt de derde beschermd tegen de risico's en gevolgen die op kunnen treden (BoF). Zolang de risico's voor een derde niet zijn ondervangen zou volgens een deel van de respondenten afgezien moeten worden van invoering van deze bevoegdheid.

De kritiek op dit onderdeel van het wetsvoorstel heeft er niet toe geleid dat de voorgestelde bevoegdheid wordt heroverwogen, ook niet waar het gaat om de mogelijkheid via het geautomatiseerde werk van een derde binnen te dringen in het geautomatiseerde werk van een target. Laatstgenoemde mogelijkheid is voor een effectieve toepassing van de bevoegdheid tot het binnendringen in een geautomatiseerd werk van essentiële betekenis. In de toelichting op deze bevoegdheid is de noodzaak daarvan nader uiteengezet; verwezen wordt naar paragraaf 3.3.4.4.6 van deze toelichting. Ook is daar nader ingegaan op het begrip geautomatiseerd werk, mede in relatie tot de reikwijdte van de bevoegdheid (bijv. de ontwikkeling van de Internet of Things). Het voorgaande neemt niet weg dat we aandacht hebben voor de door de diverse respondenten opgeworpen zorgpunten. Naar aanleiding daarvan is de voorgestelde regeling op onderdelen aangevuld. Zo wordt thans voorgeschreven dat bij het verzoek om toestemming een omschrijving van de technische risico's moet worden gegeven die verbonden zijn aan de uitoefening van de desbetreffende bevoegdheid (artikel 45, vierde lid, aanhef en onder a). Voorts is er een inspanningsverplichting opgenomen voor de diensten om het bij de uitoefening van de bevoegdheid tot het binnendringen van een geautomatiseerd werk door de diensten aangebrachte technische hulpmiddel (zoals *malware*) te verwijderen (artikel 45, zevende lid). Is dat niet mogelijk dan dient daarvan een verslag te worden gemaakt (artikel 45, zevende lid). Indien de diensten stuiten op significante kwetsbaarheden die de belangen van gebruikers op het internet kunnen schaden, dan zullen de diensten belangendragers informeren. Er kunnen echter wettelijke argumenten (zoals het beschermen van bronnen of actueel kennisniveau) of operationele redenen zijn, die openbaarmaking van kwetsbaarheden (tijdelijk) in de weg staan. Geconstateerde kwetsbaarheden hoeven niet noodzakelijkerwijs betrekking te hebben op alle gebruikers van internet, maar kunnen ook specifieke gebruikersgroepen betreffen. Belangendragers zijn dan ook niet per definitie alle gebruikers van internet, dit verschilt per casus. De diensten werken tevens nauw samen met het Nationaal Cyber Security Centrum (NCSC) en dragen zo vanuit hun expertise bij aan het vergroten van de weerbaarheid van de Nederlandse samenleving in het digitale domein. De uitoefening van de bevoegdheid wordt tot slot voorts in handen gelegd van door het hoofd van de dienst daartoe aangewezen ambtenaren die aan hem ondergeschikt zijn; onderkend wordt dat de feitelijke uitvoering van deze bevoegdheid bijzondere specialistische kennis vergt en uitsluiten in handen van daartoe gekwalificeerd

personeel moet worden gelegd (artikel 45, zesde lid). Zij zullen dan ook primair de input leveren bij de omschrijving van de technische risico's zoals hiervoor gememoreerd.

12.2.5 De medewerkingsplicht bij ontsleuteling van communicatie

In de huidige wet is reeds voorzien in een medewerkingsplicht bij de (uitoefening van de bevoegdheid van de diensten tot) ontsleuteling van versleutelde gegevens; gewezen wordt op de artikelen 24, derde lid (in het kader van uitoefening bevoegdheid tot binnendringen in een geautomatiseerd werk) en 25, zevende lid (in het kader van het gericht afluisteren) van de Wiv 2002. In het wetsvoorstel is deze medewerkingsplicht in beperkte zin uitgebreid: ook waar het gaat om de uitoefening van de bevoegdheid tot onderzoeksopdrachtgerichte interceptie (artikel 48; vergelijkbaar met het huidige artikel 27 Wiv 2002) wordt thans voorzien in een medewerkingsplicht bij de ontsleuteling van met de uitoefening van deze bevoegdheid verkregen gegevens (artikel 57 van het wetsvoorstel).

Diverse partijen die hebben gereageerd hebben ernstige bezwaren tegen een medewerkingsverplichting als hier bedoeld (onder meer Privacy First, Privacy Barometer, Amnesty International). Met name wordt als bezwaar tegen de medewerkingsplicht ingebracht dat dit in strijd zou zijn met het verbod op zelfincriminatie. Uit de ontvangen reacties blijkt voorts dat er omtrent de reikwijdte van deze verplichting in diverse opzichten onduidelijkheid bestaat. Vragen die in dat verband zijn gerezen (zie onder meer de reacties van T-Mobile, Nederland ICT, MKB NL, Amnesty International, SJB/Boekx Advocaten) betreffen met name de reikwijdte van de medewerkingsplicht, zoals op wie rust de verplichting, wat is de situatie ingeval de encryptiesleutels ontbreken of onbekend zijn, maakt het wetsvoorstel het inbouwen van achterdeuren (*backdoors*) in systemen mogelijk, moet de toepassing van encryptie in netwerken worden beperkt en beveiligde journalistieke omgevingen zouden ervan moeten worden uitgezonderd?

Er wordt geen aanleiding gezien de medewerkingsplicht als zodanig te heroverwegen. Onder omstandigheden moet het voor de diensten mogelijk zijn om bij de uitoefening van de bevoegdheid tot het ontsleutelen van gegevens die men met toepassing van de bijzondere bevoegdheden als bedoeld in de artikelen 45, 47 en 48 heeft verkregen, de medewerking in te roepen van 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. De uitoefening van deze bevoegdheden is in tegenstelling tot de huidige situatie met meer waarborgen

omgeven; zo zal er voortaan altijd voorafgaande toestemming van de voor de dienst verantwoordelijke minister vereist zijn om deze medewerking in te roepen, waarbij het verzoek daartoe aan de in artikel 29, tweede lid, gestelde eisen moet voldoen. Een verleende toestemming moet vervolgens voor een rechtmatigheidstoets worden voorgelegd aan de TIB. Van strijd met het verbod op zelfincriminatie is hier bovendien geen sprake; dat verbod is relevant ingeval van een strafrechtelijk onderzoek naar een persoon die daarbij als verdachte wordt aangemerkt. De AIVD en de MIVD zijn echter niet met de opsporing van strafbare feiten belast, maar verrichten onderzoek naar – kort gezegd – dreigingen tegen de nationale veiligheid. Vanwege het veelal heimelijke karaker van dergelijke onderzoeken is het praktisch ook uitgesloten dat men zich tot een target zou wenden om mee te werken aan de ontsleuteling van versleutelde gegevens; dat zou immers de effectiviteit van dat onderzoek ernstig (kunnen) schaden.

Waar het gaat om de onduidelijkheden die men met betrekking tot de reikwijdte van de regeling constateert, wordt het volgende opgemerkt. De verplichting kan alleen worden ingeroepen jegens een persoon waarvan vermoed wordt dat deze de benodigde kennis om de gegevens te ontsleutelen bezit; in de aanvraag om toestemming zal de dienst dit dan ook dienen te onderbouwen. Voorts strekt de verplichting voor betrokkenen niet verder dan waar zijn kennis reikt. Niet voldoen aan een medewerkingsplicht is in artikel 143 van het wetsvoorstel strafbaar gesteld. Uit de medewerkingsverplichting kan geen bevoegdheid van de diensten worden afgeleid tot het (doen) inbouwen van achterdeuren in systemen om aldus toegang tot de ontsleutelde gegevens te krijgen. Ook is er geen enkele verplichting voor aanbieders van telecommunicatienetwerken- of diensten of van zogeheten Over The Top diensten (OTT-diensten) om de encryptie in hun systemen te beperken. In dit verband wordt verwezen naar het kabinetsstandpunt inzake encryptie dat op 4 januari 2016 is uitgebracht.[301] Dat laat overigens onverlet dat ingeval een aanbieder wordt verplicht tot medewerking aan een verleende toestemming tot interceptie van telecommunicatie, de desbetreffende aanbieder de desbetreffende communicatie dient te ontdoen van door hemzelf toegepaste encryptie; een dergelijke verplichting bestaat thans reeds en is neergelegd in artikel 2, aanhef en onder e, van het Besluit aftappen openbare telecommunicatienetwerken- en diensten. In de internetconsultatie (Studiecommissie Journalistieke Bronbescherming) is ook aandacht gevraagd voor het *chilling effect* dat zou kunnen optreden indien de verplichting om mee te werken aan ontsleuteling van gegevens ook betrekking zou hebben op systemen die juist functioneren dankzij het vertrouwen dat de gebruiker heeft in de veiligheid en versleuteling (zoals Publeaks). Gesteld wordt dat beveiligde journalistieke omgevingen niet gedwongen zouden moeten kunnen worden om mee te werken aan ontsleuteling. In

[301] Kamerstukken II 2015/16, 26 643, nr. 383.

de voorgestelde regeling wordt, evenals thans reeds het geval is, geen onderscheid gemaakt in wie wel en wie niet de opdracht tot medewerking kan worden gegeven. Wel is het zo dat indien het gaat om journalistieke omgevingen er grote terughoudendheid dient te worden betracht, temeer nu daar ook het in artikel 10 EVRM gegarandeerde recht op vrijheid van meningsuiting van toepassing is. In de toestemmingverlening en de toets door de TIB zal dan ook nadrukkelijk hieraan aandacht dienen te worden besteed en zal sprake dienen te zijn van een verzwaarde proportionaliteits- en subsidiariteitstoets.

12.2.6 De samenwerking met buitenlandse diensten

In het wetsvoorstel is een regeling opgenomen inzake de samenwerking met inlichtingen- en veiligheidsdiensten van andere landen (paragraaf 6.2; de artikelen 88 tot en met 90). Deze regeling is ten opzichte van de bestaande regeling in artikel 59 Wiv 2002 op verschillende onderdelen aangevuld; zo is voorzien in een procedure die moet worden doorlopen bij het aangaan van samenwerkingsrelaties, inclusief de daarbij te hanteren criteria, de verstrekking van gegevens en de verlening van technische en andere vormen van ondersteuning. Diverse respondenten, waaronder T-Mobile, Tele2, Privacy First, NJCM, Amnesty International, SpeakUp, BoF, Studiecommissie Journalistieke Bronbescherming en Internet Society Nederland, richten zich op (diverse aspecten) van de drie genoemde onderwerpen, in het bijzonder op de gegevensvertrekking aan buitenlandse diensten en het verlenen van technische en andere vormen van ondersteuning.

Waar het gaat om het aangaan van samenwerkingsrelaties en de in artikel 86 voorziene weging wordt onder meer opgemerkt dat de opgenomen criteria vaag en moeilijk toetsbaar zijn (T-Mobile); zo zou het criterium respect voor mensenrechten specifieker moeten worden ingevuld (Amnesty International). Ook is naar voren gebracht dat in de memorie van toelichting zou moeten worden opgenomen dat bij de beoordeling van de samenwerkingsrelatie expliciet aandacht wordt besteed aan de waarborgen die worden gesteld aan gegevensverwerking, opslag en vernietiging van gegevens bij de ontvangende buitenlandse dienst (CTIVD). Erkend wordt dat de in artikel 88 opgenomen criteria, waaraan in ieder geval moet worden getoetst, noodzakelijkerwijs een abstract karakter hebben. Deze criteria dienen immers een veelheid van situaties te worden toegepast, waarbij ze bovendien in onderlinge samenhang dienen te worden gewogen, waarbij niet is gezegd dat ze onderling uitwisselbaar zouden zijn. De weging is echter geen mathematische exercitie. De genoemde criteria zijn de criteria waaraan *in ieder geval* dient te worden getoetst. Andere relevante (en voor de diensten kenbare) factoren, zoals bijvoorbeeld de voor de buitenlandse dienst geldende wet- en regelgeving

kunnen en zullen in de te maken afweging dienen te worden betrokken, zeker indien deze inzicht geven in bijvoorbeeld aan die dienst toekomende bevoegdheden, de verwerking van gegevens en het op de dienst uitgeoefende toezicht.

Waar het gaat om de gegevensverstrekking aan buitenlandse diensten door de AIVD en MIVD spreken diverse respondenten zich uit tegen verstrekking van (grote hoeveelheden) ongeëvalueerde gegevens aan buitenlandse diensten. Voor sommige is het onduidelijk waarom dit zou moeten plaatsvinden (zie Tele2, Privacy First), anderen wijzen op de risico's van verstrekking van ongeëvalueerde gegevens, bijvoorbeeld indien deze bedrijfsvertrouwelijke informatie bevat of zicht geeft op bronnen van journalisten (zie T-Mobile, Amnesty International); voor burgers is het niet voorzienbaar wat de gevolgen van een dergelijke gegevensverstrekking kunnen zijn (BoF). Nederland heeft echter een verantwoordelijkheid naar haar burgers toe (BoF). Verstrekking zou alleen moeten plaatsvinden als kenbaar is wat er wordt verstrekt (zie o.m. Internet Society NL). Onduidelijk is of en zo ja welke beperkingen aan een dergelijke verstrekking worden gesteld. Hoe wordt op het gebruik van de gegevens door de buitenlandse dienst toezicht gehouden? Ook is in de consultatie er op gewezen dat in de memorie van toelichting niet is ingegaan op hetgeen de Nederlandse diensten doen met gegevens die zij van buitenlandse diensten hebben verkregen met overschrijding van hun bevoegdheden (NJCM).

In paragraaf 6.3.3. van de memorie van toelichting is de voorgestelde regeling inzake het verstrekken van gegevens aan buitenlandse diensten toegelicht. Daarbij is aangegeven dat intensieve internationale samenwerking, en daarmee ook de uitwisseling van ongeëvalueerde gegevens, onmisbaar is. In veel gevallen leidt enkel geïntegreerd internationaal onderzoek tot het tijdig onderkennen van dreigingen. Alleen door internationaal te delen, ook waar het ongeëvalueerde gegevens betreft, kunnen gegevens op waarde worden geschat. Wanneer bijvoorbeeld uit een set gegevens blijkt dat de een jihadist uit Europees land X in contact staat met een Nederlander, moet de Nederlandse dienst dit contact tijdig kunnen beoordelen. Niet kan worden gewacht tot land X zelf de gegevens heeft geëvalueerd. Een tweede situatie betreft het geval dat een Nederlandse dienst ongeëvalueerde data heeft verstrekt aan een betrouwbare buitenlandse dienst. Deze dienst houdt die data tegen zijn eigen datasets. Dit levert een andere waardering en mogelijk uitkomst op van een gegevensanalyse. Aldus kan een buitenlandse dienst een link naar een Nederlandse jihadist onderkennen, die zonder deze verstrekking onopgemerkt had kunnen blijven.
Het is inherent aan de verstrekking van ongeëvalueerde gegevens dat niet bekend is wat de inhoud daarvan is en er kan dus ook geen 100% garantie worden gegeven dat bijvoorbeeld bedrijfsvertrouwelijke gegevens niet daarin zijn opgenomen. Dat neemt niet

weg dat de diensten – gelet op de in artikel 89, eerste lid, neergelegde criteria een inspanningsverplichting hebben het risico daarop zoveel mogelijk te minimaliseren. Nu het gaat om verstrekking van door de diensten zelf vergaarde gegevens, is op voorhand een aantal zaken reeds duidelijk, zoals de bron waaruit de gegevens zijn verkregen e.d. Daarnaast is het – afhankelijk van de soort gegevens die het betreft – soms mogelijk via een filter aan Nederland gerelateerde gegevens uit te filteren; denk daarbij aan het uitfilteren van telefoonverkeer waarbij het internationaal toegangsnummer (+31) voor Nederland is gebruikt of IP-adressen die door ICANN[302] en RIPE NCC[303] aan Nederlandse ISP-s of specifieke gebruikers(organisaties) zijn toegekend. De uitsluiting van Nederlandse gegevens bij een verstrekking aan een buitenlandse dienst brengt wel het risico met zich mee dat een link naar bijvoorbeeld een nog niet onderkende Nederlandse jihadist niet gevonden wordt. De Nederlandse gegevens zijn immers uitgesloten.
De verstrekking van gegevens aan buitenlandse diensten vindt altijd plaats onder toepassing van de derde partij-regel (zie paragraaf 3.6.3.1); ook kan verstrekking plaatsvinden onder aanvullende voorwaarden. Het toezicht op het gebruik dat door de buitenlandse diensten van de verstrekte gegevens wordt gemaakt, onttrekt zich aan het toezicht van de CTIVD; dat geldt evenzeer voor de omgekeerde situatie: ingeval gegevens worden verstrekt aan de AIVD of MIVD door een buitenlandse collegadienst zal de toezichthouder uit dat andere land evenmin in staat zijn om het gebruik van de gegevens door de AIVD en MIVD toezicht te houden. Het is dus een kwestie van vertrouwen tussen de diensten of men zich houdt aan de gemaakte afspraken ter zake van het gebruik van verstrekte gegevens. Indien dat vertrouwen wordt geschaad, is dat een factor om te komen tot een heroverweging van de samenwerkingsrelatie overeenkomstig het bepaalde in artikel 88 van het wetsvoorstel.

Inzake de samenwerking van de AIVD en/of MIVD die bestaat uit het verlenen van technische en andere vormen van ondersteuning zijn door respondenten diverse opmerkingen gemaakt. In artikel 89 is een wettelijke grondslag neergelegd voor het verlenen van technische en andere vormen van ondersteuning *door* de AIVD en/of MIVD *aan* buitenlandse diensten. De CTIVD heeft – meer ter verduidelijking - ter zake geadviseerd om in de tekst nadrukkelijker aan te geven dat het hier gaat om operationele ondersteuning. Daarnaast is de vraag gesteld welke belangen van buitenlandse diensten mogen worden behartigd door Nederlandse diensten (Amnesty International). Waar het gaat om verzoeken van buitenlandse diensten aan de AIVD en MIVD om ondersteuning wordt in de consultatie onder meer naar voren gebracht dat er ter zake in een proportionaliteitstoets moet worden voorzien en voorts dat alleen die

[302] Internet Corporation for Assigned Names and Numbers.
[303] Reseaux IP Europeens Network Coordinations Center.

bevoegdheden door de Nederlandse diensten mogen worden ingezet die de verzoekende dienst ook zelf mag inzetten.

Bij de ondersteuning als bedoeld in artikel 89 gaat het, zoals de CTIVD aangeeft, om operationele ondersteuning. Hiervan is afgezien om dat expliciet op te nemen, omdat ter zake reeds eerder in reactie op rapport nr. 22a van de CTIVD (Samenwerking van de AIVD met buitenlandse inlichtingen- en/of veiligheidsdiensten) door de minister van BZK onder verwijzing naar de wetsgeschiedenis uitdrukkelijk is aangegeven dat het daarover gaat; daar kan naar ons oordeel dan ook geen enkel misverstand ontstaan. In reactie op het door Amnesty International opgebrachte punt, wordt opgemerkt dat het hier niet zo zeer gaat om het behartigen door Nederlandse diensten van belangen van buitenlandse collegadiensten; daarvoor zijn die buitenlandse collegadiensten immers zelf verantwoordelijk (de wettekst spreekt immers niet voor niets over *door deze instanties te behartigen belangen)*. Iets anders is, dat er een belangenafweging, zoals in artikel 89, vierde lid, van het wetsvoorstel is neergelegd, dient plaats te vinden. Die belangenafweging veronderstelt dat op voorhand bekend is welk belang de buitenlandse collegadienst met de gevraagde ondersteuning nastreeft. Indien dat niet bekend is, kan die afweging niet gemaakt worden en heeft dat als gevolg dat de gevraagde ondersteuning niet kan worden verleend. In artikel 89, vijfde lid, van het wetsvoorstel is aangegeven dat in het verzoek om ondersteuning de reden waarom de ondersteuning wenselijk wordt geacht dient te worden vermeld. Indien nodig kan daarover bij de buitenlandse collegadienst aanvullende informatie worden gevraagd. Dat geldt evenzeer voor het antwoord op de vraag of ondersteuning wordt gevraagd voor een bevoegdheid die de buitenlandse collegadiensten zelf bezit; de AIVD en MIVD dienen niet mee te werken aan u-bochtconstructies van buitenlandse collegadiensten.

12.2.7 Capita selecta

Gegevensverwerking

In diverse reacties worden met betrekking tot diverse aspecten van de bevoegdheid tot gegevensverwerking opmerkingen gemaakt en vragen gesteld (onder meer Privacy First, Privacy Barometer, Nederland ICT, Microsoft, Amnesty International, Arthur’s Legal, CRvdM). Het gaat daarbij onder meer om het aspect doelbinding (en het ontbreken van een wettelijke regeling voor “hergebruik”), dataminimalisatie, bewaar- en vernietigingstermijnen en de verwerking van de opbrengst van onderzoeksopdrachtgerichte interceptie. Amnesty International vraagt aandacht voor de regeling inzake gevoelige persoonsgegevens, waarin naar haar oordeel ook de politieke gezindheid moet worden opgenomen. Een belangrijke kwestie die door met name Microsoft is opgeworpen betreft de territoriale reikwijdte, met name in relatie tot de

verplichtingen van telecommunicatie-aanbieders (belang van de vestigingslocatie van de aanbieder, de locatie van gegevens e.d.). Voorts wordt in de toelichting niet ingegaan op dataretentie.

Doelgericht verzamelen van gegevens is een belangrijk element in de verwerking van gegevens door de diensten. In artikel 18, eerste lid, van het wetsvoorstel is – evenals in het huidige artikel 12 Wiv 2002 – deze eis neergelegd; de eis van doelbinding strekt zich uit tot alle vormen van gegevensverwerking (dus niet alleen tot de verzameling maar ook tot bijvoorbeeld de verstrekking van gegevens). Dit doel moet, bijvoorbeeld bij de aanvraag van een toestemming voor de uitoefening van een (bijzondere) bevoegdheid, voldoende specifiek zijn. Zowel de TIB als de CTIVD kunnen in het kader van de aan hen opgedragen taak (toets respectievelijk toezicht) daaromtrent een oordeel vormen. Een element waaraan in de memorie van toelichting aandacht is besteed bij de toelichting van artikel 27 (beoordeling relevantie gegevens). Dit is bevestigd in rapport 38 van de CITVD.[304] Ten opzichte van het in consultatie gegeven concept-wetsvoorstel is de voorgestelde regeling aangevuld met de plicht om gegevens die met de uitoefening van bijzondere bevoegdheden zijn verzameld, zo spoedig mogelijk op relevantie te onderzoeken (artikel 27 van het wetsvoorstel); daarbij is ook voorzien in een vernietigingstermijn. Met het onderzoek op relevantie en de daaraan gekoppelde vernietigingsplicht van niet relevante gegevens wordt mede invulling gegeven aan het beginsel van dataminimalisatie. Voor een toelichting hierop wordt verwezen naar paragraaf 3.3.2.3 van de memorie van toelichting.

Amnesty International vraagt aandacht om de regeling inzake gevoelige gegevens, waarin naar haar oordeel ook politieke gezindheid zo moeten worden opgenomen. Om redenen zoals uiteengezet in paragraaf 3.2.4 kan dit verzoek niet worden ingewilligd.

Waar het gaat om de territoriale reikwijdte van het wetsvoorstel in relatie tot met name telecomaanbieders (of breder: de aanbieders van communicatiediensten), wordt het volgende opgemerkt. Evenals de huidige wet zal de nieuwe wet alleen gelding hebben op het Nederlandse territoir (inclusief de BES-eilanden); de wet heeft geen extra territoriale werking. Dat betekent dat waar in het wetsvoorstel verplichtingen (opdrachten) kunnen worden gericht aan bijvoorbeeld aanbieders van communicatiediensten deze alleen afdwingbaar zijn jegens aanbieders van communicatiediensten voor zover deze binnen de Nederlandse jurisdictie vallen. Over het algemeen zullen de aanbieders van communicatiediensten die in Nederland persoonsgegevens verwerken op grond van artikel 4 Wbp hier een vestiging dienen te hebben, hetgeen een aanknopingspunt vormt

[304] Kamerstukken II 2013/14, 29 924, nr. 105 (bijlage), p.29.

voor het uitoefenen van rechtsmacht ook waar het gaat om de verplichtingen die voortvloeien uit de Wiv 2002 of onderhavig wetsvoorstel.

Notificatie

In het wetsvoorstel is, evenals thans het geval is, voorzien in een zogeheten notificatieplicht met betrekking tot een limitatief aantal benoemde bijzondere bevoegdheden. Een aantal respondenten pleit ervoor om de notificatieplicht ook te doen gelden voor organisaties (Privacy First) en deze tevens uit te breiden tot de inzet van alle bijzondere bevoegdheden (Amnesty International).

De in het wetsvoorstel opgenomen notificatieplicht is beperkt tot een aantal bijzondere bevoegdheden en is alleen van toepassing jegens (natuurlijke) personen. Voor de (wets)historische achtergrond voor het opnemen van een notificatieregeling wordt verwezen naar hetgeen daaromtrent in het kader van de parlementaire behandeling van de Wiv 2002 is gewisseld (Kamerstukken II 1999/2000, 25 877, nr. 8, blz. 87-88). De notificatieplicht vervult een rol in het kader van het bieden van rechtsbescherming aan de burgers tegen inbreuken op enkele specifiek aan hen toekomende grondrechten. De invoering van de notificatieplicht die ook geldt voor organisaties wordt – gelet op de specifieke overwegingen die ten grondslag lagen aan de invoering van de huidige notificatieplicht - dan ook niet overwogen. Ook een verdere uitbreiding van de reikwijdte van de notificatieverplichting wordt afgewezen; een verplichting daartoe kan ook niet uit de jurisprudentie van het EHRM worden afgeleid.[305]

Verschoningsgerechtigden

In artikel 30, tweede en derde lid, van het wetsvoorstel is voorzien in een specifieke toestemmingsprocedure waar het gaat om de uitoefening van bijzondere bevoegdheden jegens een journalist, waarbij de uitoefening kan leiden tot verwerving van gegevens inzake de bron van de journalist, alsmede de uitoefening van bijzondere bevoegdheden jegens een advocaat waarbij dit kan leiden tot de verwerving van gegevens die zien op de vertrouwelijke communicatie tussen een advocaat en diens cliënt. Het eerste was (zij het beperkt tot de uitoefening van bijzondere bevoegdheden jegens een journalist *gericht op het achterhalen van diens bron*) reeds opgenomen in het in internetconsultatie gegeven concept-wetsvoorstel en bouwde voort op de regeling zoals voorzien in het bij de Tweede Kamer aanhangige voorstel van wet tot wijziging van de Wiv 2002 in verband met bronbescherming van journalisten (kamerstukken II, 2014/15, 34 027); het tweede was (nog) niet opgenomen in het concept-wetsvoorstel en ontlokte van in het bijzonder van de NOvA kritiek, omdat daarmee geen recht zou worden gedaan

[305] Zie ook Kamerstukken II 1998/99, 26 289, nrs. 4-5, pag. 204.

aan de uitspraak van de voorzieningenrechter van 1 juli 2015 (ECLI:NL:RBDHA:2015:7436). Deze uitspraak dateert echter van de dag voor de start van de internetconsultatie (2 juli 2015) en was om die reden niet in het desbetreffende concept-wetsvoorstel verwerkt. Los hiervan is in de internetconsultatie door verschillende respondenten (onder meer NOvA, FreePress Unlimited, de Vereniging voor Media- en Communicatierecht, Vrijschrift, College voor de Rechten van de Mens, CTIVD en Greenpeace) aandacht gevraagd voor de positie van verschoningsgerechtigden. Enkele respondenten vroegen zich af waarom er geen regeling is opgenomen die geldt voor *alle* verschoningsgerechtigden (onder meer Studiecommissie Journalistieke Bronbescherming, Greenpeace); andere respondenten gingen met name in op diverse aspecten van de voorziene regeling voor journalisten en de (nog op te nemen) regeling voor advocaten.

Allereerst wordt opgemerkt dat het verschoningsrecht (en daarmee ook verschoningsgerechtigde) een concept is dat uitsluitend in de strafvorderlijke context aan de orde is: immers het ziet op het recht om zich als getuige te verschonen van het beantwoorden van vragen van de rechter. In de context van de werkzaamheden van inlichtingen- en veiligheidsdiensten bestaat een dergelijk recht als zodanig niet. Niettemin zal hier het begrip verschoningsgerechtigde worde gehanteerd, omdat daarmee ook duidelijk is over wat voor soort personen het gaat.

In het wetsvoorstel is afgezien van het opnemen van een regeling die betrekking heeft op *alle* verschoningsgerechtigden. Daarbij spelen de volgende overwegingen een rol. Bij de uitoefening van bijzondere bevoegdheden komt de journalistieke bronbescherming volgens het EHRM in een democratische samenleving bijzondere betekenis toe. Zonder die bescherming zouden bronnen ervan af kunnen zien om met de pers samen te werken bij het informeren van het publiek over zaken van publiek belang. De bronbescherming vervult op dit punt een essentiële rol in onze democratie. Aan het beroepsgeheim van advocaten ligt volgens de voorzieningenrechter in diens uitspraak van 1 juli 2015 (zie hiervoor) eveneens een zwaarwegend maatschappelijk belang ten grondslag; in de brief van het kabinet aan de Tweede Kamer wordt daaraan ook nadrukkelijk gerefereerd. Het verschoningsrecht van advocaten moet worden geplaatst in de sleutel van het grondwettelijk recht op een eerlijk proces. Verdachten en andere procespartijen moeten steeds een onbelemmerde toegang tot een advocaat hebben. Advocaten vervullen op dit punt een essentiële functie ter bescherming van onze rechtsstaat. Dat is anders bij andere verschoningsgerechtigden zoals artsen en geestelijken, die de lichamelijke en geestelijke verzorging van hun cliënten voor hun rekening nemen. Dit betreft weliswaar vertrouwelijke communicatie, maar journalisten en advocaten hebben anders dan deze verschoningsgerechtigden een belangrijke rol in de borging van belangrijke aspecten van

onze democratische rechtsstaat. Dit rechtvaardigt een andere afweging voorafgaand aan de uitoefening van bijzondere bevoegdheden jegens journalisten en advocaten in de aangegeven omstandigheden.

Waar het gaat om de regeling inzake journalisten en advocaten zijn enkele specifieke opmerkingen gemaakt. De voorgestelde regeling met betrekking tot journalisten geeft enkele respondenten (in het bijzonder de Vereniging voor Media- en Communicatierecht, Studiecommissie Journalistieke Bronbescherming, en FreePress Unlimited) aanleiding tot het plaatsen van kritische opmerkingen. Een eerste, meer algemeen kritiekpunt heeft betrekking op de reikwijdte van de regeling; die zou zich namelijk moeten uitstrekken tot alle overheidsdiensten die zich bezig houden met onderzoek en opsporing. Onderhavig wetsvoorstel ziet uitsluitend op de taakuitoefening van de inlichtingen- en veiligheidsdiensten; de reikwijdte van de regeling is dan ook in die zin beperkt. Voorts wordt opgemerkt dat in het kader van de regeling met betrekking tot journalisten het begrip bron in het wetsvoorstel ten onrechte is beperkt tot die personen die gegevens hebben verstrekt onder de voorwaarde dat die verstrekking niet tot hen kan worden herleid. Terecht is opgemerkt dat niet altijd sprake hoeft te zijn van een dergelijke expliciete afspraak; de definitie van het begrip bron is daarop aangepast. VMC merkt verder op dat de voorgestelde regeling (waarbij rechterlijke toestemming nodig is voor uitoefening van bijzondere bevoegdheden) impliceert dat diensten wel onderzoek mogen doen naar journalisten indien dat niet gericht is op het achterhalen van de bron. Dat is juist. In dit kader wordt door VMC opgemerkt dat in de gevallen dat de bevoegdheidsuitoefening niet gericht is op het achterhalen van de bron van een journalist, er bij onderzoek van de communicatiegegevens van een journalist gegevens beschikbaar kunnen komen die herleidbaar zijn naar een bron. Dat kan dan niet meer ongedaan gemaakt worden. Het recht op bronbescherming wordt daarmee tot een wassen neus gemaakt. Hieromtrent wordt het volgende opgemerkt. Naar aanleiding van het advies van de Afdeling advisering van de Raad van State is er thans in voorzien dat in het geval de uitoefening van bijzondere bevoegdheden jegens een journalist *ertoe kan leiden* dat gegevens worden verworven inzake de bron van een journalist tussenkomst van de Rechtbank Den Haag is vereist. Dus de regeling is niet meer – zoals in het concept-wetsvoorstel - beperkt tot de inzet van bijzondere bevoegdheden *gericht op* het achterhalen van een bron. Gelet hierop kan men nog moeilijk volhouden dat de bronbescherming tot een wassen neus is gemaakt. Een aantal opmerkingen ziet op de toets die door de Rechtbank Den Haag zou moeten worden verricht. Zo wordt een uitwerking van de wijze waarop die toets wordt verricht gemist. Voorts wordt door VMC ervoor gepleit om de toets niet bij een aantal rechters-commissarissen te beleggen maar bij de civiele kamer, waarbij ingeval van spoedeisende situaties de voorzieningenrechter een rol zou moeten krijgen. Ook zou de rechtbank de bevoegdheid moeten krijgen om

modaliteiten aan te kunnen brengen in de opsporingsmethoden (lees: uitoefening van de bijzondere bevoegdheden) of beperkingen kan aanbrengen in het af te geven materiaal. In reactie hierop wordt opgemerkt, dat - evenals nu waar het gaat om de toets achteraf door de CTIVD op de rechtmatige uitvoering van de Wiv 2002 - er geen wettelijke regeling is opgenomen over de wijze waarop die toets en die door de rechtbank moet worden verricht. Naar onze mening biedt het wettelijk kader, in het bijzonder de daarin neergelegde criteria die bij de uitoefening van bijzondere bevoegdheden moeten worden toegepast alsmede de aanvullende motiveringseisen bij een verzoek dat betrekking heeft op de inzet van een bijzondere bevoegdheid jegens een journalist (of een advocaat) in de desbetreffende gevallen, gecombineerd met de bevoegdheid om alle noodzakelijke informatie die voor een toets nodig is op te vragen, voldoende handvatten aan de rechtbank om zelf op adequate wijze aan de wijze van toetsing invulling te geven. Aan de rechtbank Den Haag wordt niet de bevoegdheid toegekend om in het kader van de toestemmingverlening modaliteiten aan te brengen in de wijze waarop bijzondere bevoegdheden zouden moeten worden ingezet (de situatie van afgeven van materiaal aan de diensten, is – anders dan in Strafvordering – bij de toepassing van de Wiv niet aan de orde). Daarmee zou de rechtbank teveel treden in de bevoegdheid en verantwoordelijkheid van de voor de diensten verantwoordelijke ministers; immers de wijze waarop een bevoegdheid zou moeten worden ingezet kent niet alleen een rechtmatigheidscomponent maar ook een van doelmatigheid en doeltreffendheid. In dit laatste kan de rechtbank niet treden. Indien de rechtbank een verzoek om toestemming afwijst, ligt het daarbij voor de hand dat dit gemotiveerd gebeurt. Het is dan aan de verantwoordelijke minister om te bezien of wordt overgegaan tot het indienen van een nieuw verzoek, dat rekening houdt met de opmerkingen van de rechtbank. Tot slot wordt opgemerkt dat in de memorie van toelichting alsnog voorzien is in een zelfstandige toelichting op de voorgestelde regeling inzake journalisten.

Zoals hiervoor reeds is aangegeven was in het internetconsultatie gegeven voorstel nog niet voorzien in een specifieke regeling inzake advocaten; de artikelen 30, derde lid, en 66, derde lid, van het wetsvoorstel voorzien daar thans in. Daarmee is de algemene opmerking van de NOvA dat er wettelijke waarborgen ontbreken geadresseerd. De NOvA maakt in haar reactie onderscheid tussen de uitoefening van bijzondere bevoegdheden jegens een advocaat (zijnde target) en jegens een derde waarbij kennis kan worden genomen van de vertrouwelijke communicatie tussen een advocaat en diens cliënt (indirect); daarbij ligt de focus primair op de uitoefening van de bevoegdheid tot interceptie van telecommunicatie (tapbevoegdheid), die ook in de kort gedingprocedure centraal stond (direct en indirect tappen), naast de problematiek van verstrekking van door de diensten verworven communicatie als hier bedoeld aan het openbaar ministerie. De in de genoemde artikelen opgenomen regelingen adresseren alle drie de aspecten, zij

het niet geheel langs de lijnen zoals gesuggereerd door de NOvA (waaronder verplichte toepassing nummerherkenningssysteem, rol voor de Orde in bepaalde situaties), waarbij echter wel een toetsende rol voor de rechtbank Den Haag is weggelegd. De regeling ziet voorts niet alleen op de zogeheten tapbevoegdheid, maar op alle bevoegdheden waarbij mogelijk kennis genomen kan worden van de vertrouwelijke communicatie tussen een advocaat en diens cliënt. Zie voor een toelichting op de onderscheiden onderdelen de paragrafen 3.3.2.5.3 en 3.6.3.1 van de memorie van toelichting.

Transparantie

In verschillende reacties (onder meer Vodafone, Privacy Barometer, Amnesty International, PowerDNS, IVIR, BoF, Google) wordt gepleit voor meer transparantie waar het gaat om de taakuitvoering van de diensten. Dat ziet deels op een transparanter, toegankelijker en begrijpelijkere wijze van toestemmingverlening (Amnesty International), maar vooral op inzicht in de (mate van) uitoefening van bijzondere bevoegdheden, bijvoorbeeld door als overheid over te gaan tot publicatie van geaggregeerde tapstatistieken dan wel bedrijven in de telecomsector toe te staan deze in hun transparency reports te publiceren.

In dit wetsvoorstel worden de bevoegdheden van de inlichtingen- en veiligheidsdiensten die inbreuk maken op de persoonlijke levenssfeer expliciet beschreven. De regering betracht maximale transparantie over de inzet van de nieuwe bevoegdheid tot onderzoeksopdrachtgerichte interceptie. Natuurlijk kan niet worden geopenbaard tegen wie of voor welk onderzoek de bevoegdheid precies wordt ingezet. Vanzelfsprekend kan de CIVD hierover wel vertrouwelijk worden geïnformeerd en kan de CTIVD op elk gewenst moment onderzoek doen naar de uitvoering van onderzoeksopdrachtgerichte interceptie en hierover in het openbaar rapporteren.

12.3 Privacy Impact Assessment (PIA)

12.3.1 Algemeen

Bij brief van 17 maart 2015[306] heeft het kabinet de Tweede Kamer geïnformeerd dat, hoewel een PIA voor de nieuwe Wet op de inlichtingen- en veiligheidsdiensten niet verplicht is[307], men ten aanzien van deze nieuwe wet op transparante wijze inzichtelijk wil maken hoe de privacyrisico's worden afgewogen. De wetgeving met betrekking tot de inlichtingen- en veiligheidsdiensten gaat immers bij uitstek over de balans tussen het

[306] Kamerstukken II 2014/15, 33 820, nr. 5.
[307] Het Toetsmodel Privacy Impact Assessment Rijksdienst is specifiek gebaseerd op de eisen die worden gesteld aan de gegevensverwerking op grond van de Wet bescherming persoonsgegevens. De verwerking van persoonsgegevens door de inlichtingen- en veiligheidsdiensten is op grond van artikel 2, tweede lid, onder b, van de werking van deze wet uitgezonderd. Het PIA toetsmodel is dan ook als zodanig niet toegesneden op de regelgeving inzake de inlichtingen- en veiligheidsdiensten.

beschermen van de nationale veiligheid en de bescherming van de persoonlijke levenssfeer van burgers. Gelet hierop – aldus het kabinet – zou er parallel aan het in consultatie geven van het concept-wetsvoorstel een PIA worden uitgevoerd door één of meer onafhankelijke experts. Met deze toezegging werd aldus voldaan aan de door diverse Kamerfracties naar voren gebrachte wens in het Algemeen Overleg dat op 10 februari 2015 was gevoerd.

De PIA is uitgevoerd door het PI.lab. Dit is een samenwerkingsverband tussen de TNO en de universiteiten van Nijmegen (Radboud Universiteit, in het bijzonder de vakgroep Digital security van het Institute for Computing and Information Sciences) en Tilburg (Tilburg University, in het bijzonder Tilburg Institute for Law, Technology and Society, TILT), ondersteund door SIDN. Het onderzoek is verricht door onderzoekers van TNO en TILT, met een interne review vanuit de Radboud Universiteit. Het onderzoek is uitgevoerd in de periode juli tot november 2015; de rapportage inzake de PIA is in januari 2016 afgerond en medio februari aan het ministerie van BZK als opdrachtgever opgeleverd. In hoofdstuk 1 van de PIA gaan de onderzoekers onder meer in op het doel en het karakter van de PIA. Het *doel*, aldus het rapport, is te komen tot een onafhankelijke beoordeling van de privacy-implicaties van het concept-wetsvoorstel, waarbij specifiek wordt beoogd inzicht te verschaffen in de relevante aspecten waar risico's voor de bescherming van privacy van burgers optreden of kunnen optreden en waaraan vanuit die achtergrond op dit moment van het wetgevingstraject of in andersoortige borging van beschermende maatregelen aandacht besteed dient te worden. Het *karakter* van de uitgevoerde PIA is niet zozeer een (juridische) privacytoets, zoals ingeval van het Toetsmodel Privacy Impact Assessment (PIA) Rijksdienst waarbij wordt vastgesteld of een wetsvoorstel of systeem voldoet aan de juridische eisen op het gebied van privacy en bescherming van persoonsgegevens, maar *een inschatting van de privacyrisico's* van de voorgestelde wettelijke regeling en van de voorgestelde wettelijke maatregelen om deze privacyrisico's te beperken. Het rapport, aldus de onderzoekers, toetst dus niet of het concept-wetsvoorstel voldoet aan de eisen van artikel 8 EVRM.[308] Het biedt een analyse van de mate waarin de privacy van burgers geraakt wordt door het wetsvoorstel en van onderdelen waar de voorgestelde normering van de bevoegdheden vragen oproept gegeven deze mate van privacyinbreuk.[309]

In het onderstaande zal worden ingegaan op de conclusies en aanbevelingen die in hoofdstuk 11 van de rapportage zijn opgenomen alsmede aan de wijze waarop daaraan in het wetsvoorstel en de memorie van toelichting aandacht is besteed. Op de daaraan

[308] In hoofdstuk 9 van de memorie van toelichting wordt ingegaan op de grondrechtelijke en mensenrechtelijke aspecten van het wetsvoorstel, waarbij ook een toets aan de eisen van artikel 8 EVRM plaatsvindt.
[309] Zie paragraaf 1.2 en 1.3 van het rapport.

ten grondslag liggende analyse, zoals deze in de hoofdstukken 2 tot en met 10 van de rapportage zijn uiteengezet, zal slechts in voorkomende gevallen worden ingegaan.

12.3.2 De conclusies en aanbevelingen van de PIA en daaraan verbonden gevolgen

12.3.2.1 Algemeen

De uitgevoerde PIA Wiv heeft een scherp karakter en de daaraan verbonden conclusies en aanbevelingen zijn dan ook soms scherp van toon. Zoals de onderzoekers ook aangeven: het onderzoek is niet zozeer gericht op wat goed is, maar op wat volgens de onderzoekers beter kan en beter moet, vanuit het oogpunt van een adequate privacybescherming. Het nadeel van een dergelijke benadering is wel dat – door niet ook systematisch de goede punten uit het wetsvoorstel te benadrukken – een te eenzijdig en negatief beeld kan ontstaan over het wetsvoorstel. De overheid dient immers een goede balans te vinden tussen privacy en veiligheid, zonder het één ondergeschikt te maken aan het ander. Dat neemt echter niet weg dat verschillende conclusies en aanbevelingen met betrekking tot diverse onderdelen kunnen worden onderschreven en dat daaraan – of in de tekst van het wetsvoorstel of in de memorie van toelichting - opvolging is gegeven.

12.3.2.2 Conclusies

In paragraaf 11.1 van de rapportage worden enkele *conclusies* getrokken. In algemene zin wordt opgemerkt dat het wetsvoorstel in diverse opzichten een geslaagde poging is om de Wiv 2002 te actualiseren, maar niet in alle opzichten. Zo wordt opgemerkt dat het wetsvoorstel een goede aanzet biedt voor het normeringskader. Daarmee doelen de onderzoekers op een kader dat de inzet van in potentie zeer ruime bevoegdheden kanaliseert in concrete gevallen waarin ingrijpen door de diensten nodig wordt gevonden. Privacyrisico's worden volgens de onderzoekers echter bij behoorlijk veel onderdelen onvoldoende onderkend, en de voorgestelde waarborgen zijn vaak niet voldoende om de risico's af te dekken. Naar het oordeel van de onderzoekers komt dit doordat aan het wetsvoorstel een aantal onjuiste aannames ten grondslag zouden liggen. Zij wijzen in dat verband op de aannames (1) dat het zonder meer goed is om bevoegdheden technologie-onafhankelijk op te schrijven, (2) dat de verwerking van verkeersgegevens (metadata) minder ingrijpend zou zijn dan de kennisneming van de inhoud, (3) dat kabelgebonden interceptie een functioneel equivalent is van draadloze interceptie en (4) dat welbekende, veelal 20^{e}-eeuwse technologieën als verrekijkers en fotocamera's nog steeds de belangrijkste technische hulpmiddelen zijn voor de diensten. In reactie hierop merken wij op, dat er naar ons oordeel op zich niets mis is met het streven naar een zo technologie-onafhankelijk mogelijk geformuleerde wet, mits

voldoende duidelijkheid wordt gegeven wat – naar de huidige stand van zaken – de reikwijdte van de diverse bevoegdheden is. Dat sluit ook aan op de jurisprudentie van het EHRM waar het gaat om de eis van voorzienbaarheid: voor de burger moet onder andere kenbaar zijn onder welke omstandigheden, met welke middelen (bevoegdheden) jegens hem activiteiten door de diensten kunnen worden ontplooid. Bezien is of de afbakening van bepaalde bevoegdheden kon worden verbeterd, dan wel de toelichting daarop zodanig kon worden geactualiseerd dat daarmee – ook naar de toekomst toe – voldoende houvast wordt geboden voor de wijze waarop de bevoegdheid kan worden uitgeoefend. In dat opzicht is de gemaakte opmerking, dat in de memorie van toelichting nog wordt aangehaakt bij 20e-eeuwse technologieën terecht. De voorbeelden zijn in de toelichting dan ook geactualiseerd. De opmerking dat uitgegaan zou zijn van de aanname dat de verwerking van verkeersgegevens (metadata) minder ingrijpend zou zijn dan de kennisneming van de inhoud (van communicatie), achten we niet juist. Reeds in het kabinetsstandpunt naar aanleiding van het rapport van de Commissie Dessens is aangegeven 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. Daaraan hebben we vervolgens ook de conclusie verbonden dat voor metadata-analyse een extra waarborg nodig is in de vorm van ministeriële toestemming. Het onderscheid tussen interceptie van kabelgebonden en niet-kabelgebonden (ether) telecommunicatie (zie ook aanname 3) is een onderwerp dat door de onderzoekers in het rapport nog verder is verdiept, met name in relatie tot de regeling van het gericht ontvangen en opnemen van telecommunicatie die zijn oorsprong of bestemming heeft in andere landen waar het gaat om militair verkeer. In de ogen van de onderzoekers is er sprake van een onterechte gelijkstelling van beide vormen van interceptie (par. 8.2.2 van het rapport). Met de onderzoekers wordt erkend dat op normatief niveau een verschil te maken is tussen kabelgebonden en niet-kabelgebonden telecommunicatie (welke mede gerelateerd is aan de privacyverwachting van de burger); in de memorie van toelichting van de in internetconsultatie gegeven versie van wetsvoorstel is dat echter niet benoemd. Dat neemt echter niet weg dat op feitelijk niveau ontwikkelingen in het telecommunicatielandschap (telecommunicatie gaat steeds meer via de kabel) plaatsvinden, die ertoe nopen dat – niet alleen bij de hier bedoelde bevoegdheid, maar evenzeer bij de bevoegdheid tot onderzoeksopdrachtgerichte interceptie bezien dient te worden of bestaande bevoegdheden op die nieuwe realiteit dienen te worden aangepast. Uiteraard moet de noodzaak daartoe wel toereikend zijn onderbouwd; waar het gaat om de uitbreiding van interceptie tot het kabelgebonden domein is in paragraaf 3.3.4.4.7.4

van deze toelichting, mede als reactie op de commentaren ter zake in het kader van de internetconsultatie, de nut en noodzaak daarvan nader uiteengezet. Waar het gaat om het militair verkeer is – mede naar aanleiding van de opmerkingen van de onderzoekers in de PIA Wiv – thans alsnog voorzien in het stellen van het toestemmingsvereiste (zie artikel 47, achtste lid, van het wetsvoorstel).

In de PIA Wiv wordt verder opgemerkt dat het – in consultatie gegeven – concept-wetsvoorstel voorts enkele andere valkuilen kent. Daarbij wordt onder meer gewezen op gekozen constructies (zoals de driefasenbenadering bij onderzoeksopdrachtgerichte interceptie), de verspreiding van het normeringskader over verschillende onderdelen en het gebruik van kruisverwijzingen. De wet zou daardoor alleen voor gespecialiseerde juristen te bevatten zijn, hetgeen ten koste zou gaan van de kenbaarheid voor de gewone burger maar ook het risico oplevert dat in het wetgevingstraject de reikwijdte van de voorstellen niet goed ingeschat kan worden. Erkend wordt dat het wetsvoorstel een complex geheel aan regels bevat; dat is haast onontkoombaar bij een wetsvoorstel dat voor vrijwel het gehele werkterrein van de diensten, inclusief het daarop van toepassing zijnde gespecialiseerde toezicht (toetsing, toezicht en klachtbehandeling), regels bevat. Dat neemt niet weg dat zowel op wetsniveau als op het niveau van de memorie van toelichting gestreefd dient te worden naar een heldere, begrijpelijke en eenduidige normstelling onderscheidenlijk een begrijpelijke en ter zake doende toelichting. In het voorliggende wetsvoorstel en de memorie van toelichting is getracht daaraan – mede aan de hand van de gedane aanbevelingen, maar ook als reactie op opmerkingen uit de internetconsultatie - invulling aan te geven. Ook is de memorie van toelichting op diverse onderdelen – waar dienstig met voorbeelden - aangevuld teneinde de betekenis van diverse onderdelen te verduidelijken.

12.3.2.3 Aanbevelingen

In paragraaf 11.2 van het rapport worden de aanbevelingen op een rij gezet, welke uit de analyses en de conclusies op de diverse onderdelen van het rapport volgen. In het onderstaande zal per aanbeveling worden aangegeven of en, zo ja, op welke wijze daaraan opvolging is gegeven.

Aan de algemene aanbeveling (1) om de structuur van de wet helderder en simpeler te maken is gevolg gegeven door de bepalingen die in algemene zin van toepassing zijn op de *verwerking* van gegevens bij elkaar in één paragraaf te plaatsen (paragraaf 3.1). Waar het gaat om de *verzameling* van gegevens zijn in paragraaf 3.2.1 diverse bepalingen die deels bij de regeling inzake bijzondere bevoegdheden en deels in een afzonderlijke paragraaf afwegingskader en verslaglegging waren voorzien (conform de regeling in de huidige wet) bij elkaar geplaatst. Daarmee wordt duidelijk dat het

afwegingskader en de verslagplicht van toepassing is ongeacht de bevoegdheid die men wil inzetten. Dit is temeer van belang nu in het wetsvoorstel de bevoegdheden die men in ieder geval bij de verzameling van gegevens mag inzetten (bronnen) in artikel 25, eerste lid, van het wetsvoorstel worden benoemd, waarmee tegelijk ook aan OSINT (open bronnen) een expliciet wettelijke basis wordt gegeven; in artikel 25, tweede lid, wordt de mogelijkheid geopend dat de voor de dienst verantwoordelijke minister ook andere bronnen aanwijst waarvan de desbetreffende dienst gebruik mag maken. In het wetsvoorstel wordt de aanduiding bijzondere bevoegdheden gehandhaafd, zij het dat het bijzondere ervan met name daarin is gelegen dat deze bevoegdheden uitsluitend mogen worden ingezet bij de uitvoering van de taken als bedoeld in artikel 8, tweede lid, onder a en d, (AIVD) en 10, tweede lid, onder a, c en e, (MIVD) van het wetsvoorstel; de bijzondere bevoegdheden kunnen, evenals thans het geval is, dus niet worden ingezet bij veiligheidsonderzoeken, de veiligheid bevorderende taak en het opstellen van dreigings- en risico-analyses in het kader van het stelsel bewaking en beveiliging. Naar aanleiding van de PIA Wiv is thans in artikel 38 van het wetsvoorstel voorzien in een regeling voor het stelselmatig verzamelen van gegevens omtrent personen uit open bronnen (OSINT); de uitoefening van deze bevoegdheid is (op vergelijkbare wijze als bij de bijzondere bevoegdheden) onderworpen aan toestemming van de betrokken minister of namens deze het hoofd van de desbetreffende dienst (met mogelijkheid van ondermandaat). De bevoegdheid tot het raadplegen van informanten is in aangepaste vorm in het wetsvoorstel opgenomen (artikel 39). In het in consultatie gegeven concept-wetsvoorstel is in de regeling inzake het verlenen van toestemming voor de uitoefening van bijzondere bevoegdheden voorzien in een specifiek toestemmingsregeling waar het de uitoefening van bijzondere bevoegdheden jegens journalisten betreft voor zover gericht op het achterhalen van hun bronnen; in dat geval dient de rechtbank Den Haag de toestemming te verlenen. Daarbij is aansluiting gezocht bij de regeling, zoals opgenomen in het bij de Tweede Kamer aanhangige wetsvoorstel tot wijziging van de Wiv 2002 (kamerstukken II 2014/15, 34 027). Naar aanleiding van het advies van de Afdeling advisering van de Raad van State is de regeling aangepast: toestemming van de rechtbank is voortaan vereist in alle gevallen waarbij de inzet van bijzondere bevoegdheden jegens journalisten kan leiden tot de verwerving van gegevens inzake bronnen. Daarnaast is het wetsvoorstel ten opzichte van de consultatieversie aangevuld met een regeling voor de uitoefening van bijzondere bevoegdheden jegens advocaten, voor zover daarbij de vertrouwelijke communicatie tussen een advocaat en diens cliënt in het geding is (inclusief een regeling met betrekking tot het verstrekken van dergelijke gegevens aan het openbaar ministerie; dit laatste is niet geregeld in artikel 30 van het wetsvoorstel, maar in artikel 66, derde lid). Ook hier wordt de rechtbank Den Haag belast met de toestemmingverlening; ook waar het gaat om voorgenomen verstrekking

door de diensten van communicatie als hier bedoeld aan het openbaar ministerie. Naar aanleiding van het betoog in paragraaf 4.6.3 van de PIA Wiv is voorts een algemene bepaling opgenomen met de strekking dat gegevens die verkregen zijn door de uitoefening van een bijzondere bevoegdheid zo spoedig mogelijk op relevantie moeten worden onderzocht; gegevens waarvan is vastgesteld dat ze niet relevant zijn, dienen ter worden vernietigd. Dit onderzoek dient binnen een bepaalde periode (een jaar, met de mogelijkheid van een eenmalige verlenging van zes maanden) plaats te vinden, waarna de (niet op relevantie onderzochte) gegevens dienen te worden vernietigd (artikel 27, eerste en derde lid). Daarbij is dus gedeeltelijk aansluiting gezocht bij het in de PIA Wiv geformuleerde tekstvoorstel (en deels invulling gegeven aan aanbeveling 12 onder c van de PIA Wiv).

Aanbeveling 3 om een bepaling op te nemen over gegevensbescherming *by design* en *by default*, zoals voorgesteld, is niet overgenomen. Naar ons oordeel kan een dergelijke bepaling aangewezen zijn, indien de verantwoordelijke voor de gegevensverwerking zelf veel ruimte is gelaten om met het oog op dienst taak- of doelstelling de wijze waarop hij gegevens verwerkt (in zijn diverse aspecten) invulling te geven en daarbij de in geding zijnde privacyrisico's te minimaliseren. In het wetsvoorstel is echter een specifiek kader voor diverse aspecten van gegevensverwerking opgenomen, waarbij in de afweging de privacyrisico's – uitgewerkt in diverse waarborgen - reeds zijn meegewogen. Uiteraard bestaat op onderdelen de noodzakelijke beleidsruimte, bijvoorbeeld bij de verstrekking van gegevens, maar in de wet worden de grenzen getrokken. Daarom kan naar ons oordeel volstaan worden met een bepaling, waarbij het hoofd van de dienst de zorgplicht opgelegd krijgt om de technische, personele en organisatorische maatregelen in verband met de verwerking van gegevens in overeenstemming zijn met hetgeen bij of krachtens de wet is bepaald (artikel 24, eerste lid).

De PIA Wiv doet vervolgens een aantal aanbevelingen (4 tot en met 9) ter zake van onderdelen van het wetsvoorstel waarbij men de privacyrisico's onaanvaardbaar groot acht. Daarvan is sprake indien, aldus de PIA Wiv, de noodzaak niet is aangetoond en ook niet aannemelijk is te maken, ook niet als er zwaardere waarborgen zouden worden voorgesteld. Het betreft hier een zestal ongelijksoortige onderwerpen, waarbij naar ons oordeel op onderdelen wel degelijk aannemelijk is te maken dat de voorgestelde maatregelen noodzakelijk zijn en met aanpassingen op onderdelen ook aanvaardbaar. Hierop zal thans worden ingegaan.

Aanbeveling 4 stelt dat er geen DNA-databank bij de diensten moet worden opgezet; naar het oordeel van de onderzoekers is dit de ingrijpendste uitbreiding van bevoegdheden (par. 6.6 PIA Wiv). Naar het oordeel van de onderzoekers zouden

daarvoor geen klemmende redenen kunnen worden aangevoerd; tegelijkertijd wordt echter – voor zover er een *pressing social need* kan worden aangetoond – wel degelijk de mogelijkheid opengelaten dat dit voor een specifieke groep (zelfmoordterroristen) met een maximale bewaartermijn wel mogelijk zijn. Naar ons oordeel bestaat er wel degelijk een noodzaak om DNA-profielen gedurende een bepaalde periode vast te leggen, niet alleen ter identificatie en verificatie, maar ook met het oog op toekomstige identificatie (dat inderdaad iets anders is dan verificatie). De memorie van toelichting is op dat punt aangevuld; zie paragraaf 3.3.4.4.4. Voorts is de regeling aangescherpt en wel in die zin, dat binnen drie maanden na verwerving van het celmateriaal (met de mogelijkheid van eenmalige verlenging voor eenzelfde periode) het DNA-profiel dient te worden opgesteld; vervolgens dient binnen drie maanden daarna het celmateriaal te worden vernietigd.

Aanbeveling 5 van de PIA Wiv gaat in op de in het wetsvoorstel voorziene bevoegdheid van de diensten om – in voorkomende gevallen – via het geautomatiseerde werk van een derde bij het geautomatiseerde werk van het doelwit te komen. De onderzoekers stellen dat het feit dat doelwitten van de diensten hun computer over het algemeen goed beveiligen nooit de privacyrisico's rechtvaardigen van het hacken van computers van onverdachte burgers in hun omgeving. Het introduceren van deze bevoegdheid wordt in de PIA Wiv dan ook afgewezen (onaanvaardbare privacyrisico's die ook niet te adresseren zouden zijn). Ook in de internetconsultatie (zie hiervoor) zijn door enkele respondenten, zoals BoF, zorgen geuit over de potentiële reikwijdte van de voorgestelde bevoegdheid en de daaraan verbonden risico's voor de desbetreffende derden. Door sommigen is zij zelfs in het geheel afgewezen. Wij erkennen dat het binnendringen in een geautomatiseerd werk moet worden gerekend tot de in potentie meest inbreukmakende bijzondere bevoegdheden. In verband hiermee is de voorgestelde wettelijke regeling ten opzichte van het voorstel in de consultatieversie op onderdelen aangescherpt; voorts zal de door de minister verleende toestemming onderworpen worden aan de rechtmatigheidstoets van de nieuwe commissie Toezicht Inzet Bevoegdheden (TIB) (zie artikel 36, eerste lid, van het wetsvoorstel). Zonder een positief oordeel van deze commissie kan geen uitvoering worden gegeven aan de verleende toestemming; deze vervalt dan van rechtswege. In de toelichting op artikel 45 (paragraaf 3.3.4.4.6) is nader ingegaan op de noodzaak van het binnendringen van een geautomatiseerde werk van een target via dat van een derde. Voorts wordt daarbij ingegaan op enkele andere wijzigingen, die ertoe strekken de uitoefening van de bevoegdheid met meer waarborgen te omgeven.

In aanbeveling 6 wijzen de onderzoekers de verplichting van aanbieders van niet-openbare communicatie om zelf de kosten te dragen voor het aftapbaar maken van hun

systemen af. Zoals hiervoor bij de bespreking van de reacties uit de internetconsultatie reeds is aangegeven, wordt er thans in voorzien dat deze kosten naar redelijkheid door de overheid zullen worden vergoed (zie artikel 53, zevende lid). Daarmee worden eventuele door de onderzoekers gesignaleerde privacyrisico's op dit punt (par. 8.1.3, blz. 124) naar onze mening adequaat weggenomen; overigens zou ook los hiervan op de overheid de plicht rusten om in overleg met de aanbieder te bezien op welke wijze door deze ook in technische zin aan de desbetreffende last uitvoering zou moeten worden gegeven. Met de voorgestelde regeling kan naar ons oordeel worden afgezien van de door de onderzoekers aanbevolen impact-analyse.

Aanbeveling 7 betreft de reikwijdte van de definitie van communicatieaanbieders, die naar de mening van de onderzoekers niet moet uitstrekken tot diensten die externe opslag van gegevens aanbieden. Dat betreft dan die diensten van externe opslag die *niet* worden aangeboden in het kader van een communicatiefunctionaliteit en daarmee onlosmakelijk zijn verbonden. Artikel 54 van het concept-wetsvoorstel geeft de diensten de bevoegdheid zich te wenden tot een aanbieder van een communicatiedienst met de opdracht gegevens te verstrekken die betrekking hebben op de inhoud van de telecommunicatie van een gebruiker die door de aanbieder *als onderdeel van de door hem verleende communicatiedienst* ten behoeve van een gebruiker is opgeslagen. Dat impliceert volgens onderzoekers dat gegevens die anders dan in het kader van een verleende communicatiedienst door een derde ten behoeve van een gebruiker worden opgeslagen, buiten de reikwijdte van deze bevoegdheid vallen. Het gaat hier ook niet om (tele)communicatie waarop de bijzondere bevoegdheden van paragraaf 3.2.5.6 zien. In die zin wordt dat deel van de aanbeveling onderschreven. De vergelijking met zaken die traditioneel onder bescherming van het huisrecht zouden vallen, nl. indien deze fysiek in de woning van een onderzoekssubject zouden bevinden, gaat naar onze mening niet op. De bestanden zijn juist niet in de woning opgeslagen, maar bijvoorbeeld via de externe opslag van een clouddienst of opslag via een applicatie op een smartphone. De benadering van dit type dienst vanuit het huisrecht, zoals de onderzoekers voorstaan (Zie par. 8.1.1, blz. 120), gaat naar onze mening te ver; de herziening van de Wiv 2002 is overigens ook niet de plaats om een fundamentele discussie over de reikwijdte van het huisrecht te voeren. Bij het opvragen van gegevens als hier bedoeld – los van het feit of deze nu wel of niet verbonden zijn aan de verlening van een communicatiedienst - is van een activiteit die zich richt op wat *in* een woning plaatsvindt geen sprake. Temeer nu dergelijke opslag ook plaatsvindt om juist ongeacht de locatie waar men zich bevindt, te kunnen worden benaderd. Nu het voor een goede taakuitvoering van de diensten noodzakelijk is ook onder voorwaarden toegang te kunnen krijgen tot gegevens die in andere vormen van cloud-opslagdiensten dan die welke verbonden zijn aan een verleende communicatiedienst, wordt ter zake in artikel 54, eerste lid, onder b, van het

wetsvoorstel in een afzonderlijke bijzondere bevoegdheid voorzien. In paragraaf 3.3.4.4.7.5 van de memorie van toelichting wordt de regeling – ook op dit onderdeel – toegelicht.

In aanbeveling 8 geven de onderzoekers aan dat de verstrekking van ongeëvalueerde gegevens aan buitenlandse diensten een aantasting van de essentie van het recht op privacy en niet voldoet aan het subsidiariteitsbeginsel. Indien een samenwerking met een buitenlandse dienst is overeengekomen, zouden de gegevens niet ongeëvalueerd verstrekt mogen worden, maar zou de Nederlandse dienst, namens of gezamenlijk met de buitenlandse dienst, de gegevens zelf moeten analyseren met het oog op het doel waarvoor de buitenlandse dienst die gegevens verzoekt. Dit zou ertoe moeten leiden dat de buitenlandse dienst alleen die gegevens verstrekt krijgen die passen bij het doel waarvoor ze verstrekt worden. Wij ontkennen niet dat de verstrekking van ongeëvalueerde gegevens aan buitenlandse collegadiensten vanuit privacyperspectief bezien niet onproblematisch is. De realiteit is echter dat om als land hoofd te kunnen bieden aan dreigingen die een internationaal karakter hebben en zich niet aan landsgrenzen storen, samenwerking met buitenlandse diensten is aangewezen; dat ziet in het bijzonder op de bestrijding van terrorisme en cyberdreigingen. Dat kan, zoals ook ter toelichting op het bepaalde in artikel 88 en 89 is gesteld, verschillende vormen aannemen; onder andere in de vorm van de verstrekking van ongeëvalueerde gegevens. De samenwerking met buitenlandse collegadiensten is gebaseerd op het *quid pro quo*-principe (voor wat, hoort wat); men krijgt als dienst pas gegevens, als men zelf ook gegevens verstrekt. Indien men hiervan afziet, betekent dat een belangrijke informatiebron wegvalt. Dan rijst de vraag of men het daarmee gepaard gaande risico voor de nationale veiligheid wil lopen. Een buitenlandse dienst heeft een eigen informatiepositie. Door ongeëvalueerde data te verstrekken kan de buitenlandse dienst deze data tegen zijn eigen datasets aanhouden, waardoor een voor de Nederlandse diensten ongekende dreiging onderkend kan worden. In paragraaf 6.3.3 van de memorie van toelichting is nader op de gegevensuitwisseling met buitenlandse diensten ingegaan; zie overigens ook hoofdstuk 1 van de memorie van toelichting.

Aanbeveling 9 ziet op artikel 55, eerste lid, van het concept-wetsvoorstel (nu: artikel 69 van het wetsvoorstel). Naar het oordeel van de onderzoekers zouden "verouderde of onbetrouwbare gegevens" niet verstrekt mogen worden aan buitenlandse diensten. Het gaat immers om gegevens die, aldus de onderzoekers, hoogstwaarschijnlijk niet relevant zijn of waarvan de relevantie (vanwege de onbetrouwbaarheid) niet kan worden vastgesteld, en waarvan niet kan worden gecontroleerd op welke manier de buitenlandse dienst er gebruik van zal maken. Artikel 55, tweede lid, onder a, van het concept-wetsvoorstel (nu: artikel 69, tweede lid, onder a van het wetsvoorstel) zou volgens

onderzoekers integraal moeten komen te vervallen. Naar aanleiding hiervan merken we het volgende op. "Onbetrouwbaar" en "verouderde" zijn ongelukkig gekozen termen. Het betreft hier oude gegevens of gegevens waarvan de juistheid niet kan worden vastgesteld. De diensten gaan geen onbetrouwbare gegevens delen. De verstrekking van gegevens waarvan de juistheid niet vaststaat kan evenwel tot doel hebben om in gezamenlijkheid de betrouwbaarheid vast te stellen. Dit is bijvoorbeeld het geval als de betrouwbaarheid van een nieuwe bron nog niet is vastgesteld en slechts geëvalueerd kan worden door zijn bevindingen te (laten) verifiëren door het te toetsen aan gegevens waarvan de betrouwbaarheid wel vast staat. Dit komt bij het werken met menselijke bronnen (HUMINT) veelvuldig voor. Oude gegevens kunnen nog wel betrouwbaar zijn, maar 'verouderde' nooit. Dat is intrinsiek aan het begrip 'verouderd' (achterhaald, gedateerd, passé). Indien er RFI's (*requests for information*) van andere diensten komen, en het betreffen oude gegevens, dan is het de plicht van de diensten om de relevantie van die oude gegevens eerst te duiden. Ook de diensten zelf hebben er – in verband met de mogelijke terugkoppeling - geen belang bij om verkeerde gegevens te verstrekken. De mitigerende maatregel om te voorkomen dat diensten gebruik maken van oude informatie zonder de juiste waarde te hechten aan de ouderdom is juist gelegen in de verplichte ouderdomsaanduiding. Oude gegevens kunnen bijvoorbeeld van grote waarde zijn wanneer een conflict na enige jaren van luwte weer oplaait. Het tweede vereiste, namelijk dat ten aanzien van de desbetreffende persoon sindsdien geen nieuwe gegevens zijn verwerkt, geeft aan dat dit artikel enkel en alleen geëvalueerde gegevens betreft. Men heeft immers een oordeel moeten vellen over de juistheid en de precieze personen die in de te verstrekken gegevens worden genoemd. Ongeëvalueerde gegevens vallen buiten de strekking van dit artikel en worden, ingeval verstrekking aan een buitenlandse dienst wordt overwogen, conform artikel 64, tweede lid (bij een verstrekking in het kader van de eigen goede taakuitvoering van een dienst) of artikel 89, tweede lid (in het kader van een samenwerkingsrelatie met de desbetreffende buitenlandse collegadienst) voor toestemming aan de minister voorgelegd.

In de aanbevelingen 10 tot en met 15 van de PIA Wiv worden met betrekking tot enkele onderdelen aanbevelingen gedaan om tot een ingrijpende versterking van de waarborgen te komen om de grote privacyrisico's te kunnen rechtvaardigen.

Aanbeveling 10 ziet op versterking van het toezicht, dat niet alleen onafhankelijk maar ook effectief moet zijn. Aanbevolen wordt de CTIVD ook buiten de klachtbehandeling om bindend adviesrecht te geven. De aanbeveling in de PIA Wiv komt er eigenlijk op neer, dat alsnog uitvoering wordt gegeven aan een aanbeveling van de Commissie Dessens om de CTIVD de bevoegdheid te geven tot een (onmiddellijke) bindende rechtmatigheidstoets. Dit is eerder door het kabinet afgewezen. Mede naar aanleiding

van de vele reacties in de internetconsultaties die het gebrek aan onafhankelijk toezicht hekelden, stelt de regering in onderhavig wetsvoorstel voor om te voorzien in een TIB. Zie hetgeen daaromtrent in paragraaf 12.2.3 van deze memorie van toelichting is gesteld.

Aanbeveling 11 gaat in op de bevoegdheid van de diensten tot het raadplegen van informanten (ook wel aangeduid als de 'algemene' bevoegdheid tot het opvragen van gegevens). In artikel 39 van het wetsvoorstel is deze bevoegdheid geregeld. Op de uitoefening van deze bevoegdheid zijn de in artikel 26 van het wetsvoorstel neergelegde eisen inzake proportionaliteit en subsidiariteit van toepassing verklaard (het algemeen normeringskader). Waar het gaat om geautomatiseerde toegang tot gegevens bij derden, die op basis van vrijwilligheid daartoe aan de diensten toegang verlenen, is in artikel 39, vierde lid, de geautomatiseerde toegang nader uitgewerkt. Zie voorts paragraaf 3.3.4.3 van de memorie van toelichting.

In aanbeveling 12 worden diverse voorstellen gedaan met betrekking tot het regime voor opslag en vernietiging van gegevens; dat regime zou met aanzienlijk sterkere waarborgen moeten worden omkleed. Het betreft hier de bewaartermijnen, het zo spoedig mogelijk op relevantie onderzoeken van verzamelde gegevens en het vernietigen van niet relevante gegevens, het bewaren van verwijderde (maar nog niet vernietigde) gegevens en een maximale opslagtermijn voor relevante gegevens. Naar aanleiding van deze aanbeveling is nogmaals naar de bewaartermijn van verschillende gegevens gekeken, mede in combinatie met de voorgestelde algemene bepaling inzake een onderzoeksplicht op relevantie. Een en ander heeft geleid tot het opnemen van een regeling zoals voorgesteld in artikel 27; kortheidshalve wordt verwezen naar de toelichting daarop. Waar het gaat om het bewaren van DNA-profielen wordt een afwijkende bewaartermijn van vijf jaar voorgesteld (met een verlengingsmogelijkheid tot maximaal 30 jaar in totaliteit); waar het gaat om de met toepassing van de onderzoeksopdrachtgerichte interceptie geldt een bewaartermijn van drie jaar. Waar het gaat om de verwijderde gegevens (waaraan aanbeveling 12 onder c refereert) gaat het om gegevens die door de diensten eerder zijn gebruikt in het kader van het reguliere bedrijfsproces (het betreft hier dan ook geëvalueerde gegevens); deze gegevens zijn onderworpen aan het regime van de Archiefwet 1995 en kunnen niet zonder meer worden vernietigd (zie artikel 21 van het wetsvoorstel). Dat is slechts mogelijk aan de hand van op grond van de Archiefwet 1995 vastgestelde selectielijst; zie ook hetgeen in paragraaf 3.2.5 is gesteld. Op grond van artikel 20, eerste lid, van het wetsvoorstel bestaat voor de diensten reeds de verplichting om gegevens die, gelet op het doel waarvoor ze zijn verwerkt, geen betekenis hebben *of hun betekenis hebben verloren*, te verwijderen. Het stellen van een maximale bewaartermijn voor relevante gegevens

achten we mede gelet op deze verplichting dan ook niet aangewezen. Het dient tot het reguliere bedrijfsproces van de diensten te horen dat doorlopend wordt bezien of gegevens die niet meer relevant zijn worden verwijderd.

In aanbeveling 13 wordt erop gewezen dat het binnendringen in een geautomatiseerd werk inmiddels de zwaarst denkbare inbreuk is op de privacy en dan ook met het zwaarst mogelijke toezicht dient te worden omkleed. In dit kader acht men voorafgaande toestemming van de rechtbank aangewezen om de privacyrisico's te kunnen rechtvaardigen; voorts zou de aanbeveling van de Commissie Dessens voor een onmiddellijke toetsing door de CTIVD moeten worden ingevoerd. Zoals al eerder is aangegeven, wordt in het wetsvoorstel thans voorzien in een onafhankelijke bindende toets door de TIB (een commissie bestaande uit drie leden, waarvan in ieder geval twee leden tenminste zes jaar als rechter werkzaam zijn of zijn geweest); naar ons oordeel vormt de TIB dan ook een gelijkwaardig alternatief voor een rechterlijke toets, in ieder geval vanuit EVRM-perspectief bezien.

In aanbeveling 14 wordt, waar het om de voorgestelde regeling inzake onderzoeksopdrachtgerichte interceptie gaat, aangegeven dat de toets op rechtmatigheid naar het oordeel van de onderzoekers vooral ook *tijdens* het uitvoeringsproces doorlopend moeten worden uitgevoerd. Onmiddellijk toezicht door de CTIVD vormt aldus de onderzoekers hier een belangrijke, en moeilijk vervangbare, waarborg. Dit voorstel komt materieel overeen met hetgeen men met betrekking tot het binnendringen van een geautomatiseerd werk heeft voorgesteld (zie hiervoor); kortheidshalve wordt naar de daar gegeven reactie verwezen. Daarnaast wordt opgemerkt dat de CTIVD – evenals nu – reeds de bevoegdheid heeft om de betrokken ministers gevraagd en ongevraagd in te lichten en te adviseren omtrent de door haar geconstateerde bevindingen (zie huidig artikel 64, tweede lid, onder b, Wiv 2002; artikel 97, derde lid, onder b, van het wetsvoorstel); niet alleen naast, maar ook tijdens een lopend onderzoek. Op deze wijze kan de minister tussentijds van geconstateerde onrechtmatigheden in de uitvoering op de hoogte worden gebracht, zodat deze in staat is daarop in te grijpen. De CTIVD kan desgewenst de minister verzoeken om haar bevindingen ter kennis van de Staten-Generaal te brengen. Naar ons oordeel is op deze wijze effectief toezicht verzekerd op het gehele proces.

In de PIA Wiv wordt in aanbeveling 15 de tweefasenaanpak van prof. dr. B.P.F. (Bart) Jacobs aanbevolen in plaats van het – aldus de onderzoekers – papieren onderscheid in drie stappen, die in de praktijk diffuus zouden zijn en snel door elkaar heen kunnen lopen. De eerste fase ziet dan op een vluchtige en dus niet systematisch inhoudelijke blik naar de relevantie van de gegevens; in de tweede fase – van stelselmatigheid - richt zich

het onderzoek op de aldus gefilterde en dus meer relevante gegevens. Wij zien geen aanleiding om op deze fasering terug te komen. Ook de uitwerking van voorstel van Bart Jacobs in zijn artikel "Select while you collect, Over de voorgestelde interceptiebevoegdheden voor inlichtingen- en veiligheidsdiensten" (NJB 29 januari 2016, afl. 4, p. 198) noopt naar ons oordeel niet tot een aanpassing van het stelsel als zodanig. Jacobs geeft aan dat het in het wetsvoorstel neergelegde stelsel uitgaat van het beginsel *collect before you select*; geïntercepteerde gegevens komen in een grote bak en mogen drie jaar bewaard blijven; de beperkingen in het wetsvoorstel, aldus Jacobs, richten zich op de soorten onderzoeken die op deze bak uitgevoerd mogen worden. De methodiek *select before you collect*, welke veronderstelt dat van te voren bekend is waar naar gezocht wordt, acht hij in de wereld van inlichtingen- en veiligheidsdiensten niet realistisch. Zijn voorstel typeert hij als *select while you collect*: verzamelen en selecteren (*searchen*) gaan hand in hand. Aan de door Jacobs voorgestelde uitgangspunten wordt met de driefasenaanpak uit het wetsvoorstel op hoofdlijnen recht gedaan: interceptie en search (gericht op interceptie) zijn immers met elkaar verweven – ook in het wetsvoorstel - en ook daarvan is het doel om tot een optimalisatie van het interceptieproces te komen; aan de hand van (technische) filters worden irrelevante gegevens direct uitgefilterd en weggegooid. Het principe dat ten grondslag ligt aan de methodiek van Jacobs wordt daarom op hoofdlijnen onderschreven. Thans wordt gewerkt conform het gestelde in paragraaf 3.3.4.4.7.4, waarin is opgenomen dat bij de onderzoeksopdrachtgerichte interceptie enkel data wordt verworven die ten goede komt aan de onderzoeksopdrachten en waardoor direct een forse datareductie plaatsvindt.

Jacobs lijkt daarin echter verder te willen gaan, dan wat wij gelet op de taakuitvoering van de diensten noodzakelijk achten; met name het kunnen beschikken (voor een periode van maximaal drie jaar) over historische(meta)data door de diensten weegt voor ons in deze zwaar. Jacobs komt vanuit de optiek om de werkwijze van de diensten toch nadrukkelijk volgens de *select while you collect* systematiek als waarborg te laten verlopen met een drietal suggesties. Het nadrukkelijk benadrukken van de voorwaarde van proportionaliteit en noodzakelijk in het interceptieartikel zelf achten wij onnodig; dat is een algemene eis, die ook bij de toepassing van artikel 48 gewoon geldt. De tweede suggestie om nadrukkelijk de *select while you collect* werkwijze in de toelichting te beschrijven – in contrast met de 'grote bak'-systematiek – is naar ons oordeel gelet op wat we hiervoor en in paragraaf 3.3.4.4.7.4 hebben gesteld niet aan de orde. Waar het gaat om het toezicht, namelijk dat de CTIVD – evenals bij gerichte interceptie – de *select while you collect* werkwijze als maatstaf hanteert, zal deze zich uiteindelijk (nu haar toezichthoudende taak zich richt op de rechtmatige uitvoering van de wet) dienen te richten naar het stelsel en de invulling zoals dat uiteindelijk door de wetgever daaraan

wordt gegeven. Voor de overige in de aanbeveling genoemden aspecten wordt verwezen naar hetgeen daaromtrent eerder in deze toelichting is gesteld.

In de aanbevelingen 16 tot en met 24 van de PIA Wiv worden met betrekking tot enkele onderdelen verbeteringen voorgesteld, die – hetzij in de waarborgen, hetzij in de formulering of afbakening van bepalingen – nodig zijn om de privacyrisico's te rechtvaardigen.

In aanbeveling 16 wordt aanbevolen om alle bevoegdheden waarbij van buitenaf kennis wordt genomen van wat zich in een woning afspeelt te binden aan dezelfde waarborgen als het betreden van woningen. Eerder zijn we in reactie op aanbeveling 7 ingegaan op de problematiek van de *reikwijdte van het huisrecht* in artikel 12 Grondwet en dat de herziening van de Wiv 2002 niet de plek is om daar een principiële discussie over te voeren. We zien dan ook thans geen aanleiding om vooruitlopend op een eventuele discussie daarover reeds op voorhand in de sfeer van waarborgen daar – waar het de genoemde bevoegdheden betreft – aansluiting bij te zoeken.

In aanbeveling 17 wordt gesteld dat privacy in de publieke ruimte meer dan voorheen juridische bescherming nodig heeft. De ongewijzigde regeling in het wetsvoorstel van observatie (buiten woningen) doet, aldus de PIA Wiv, geen recht aan de gewijzigde realiteit. De wetgever zou ter zake sterkere waarborgen moeten overwegen, met name waar door combinatie van hulpmiddelen en/of langdurige observatie een cumulatief beeld kan ontstaan van iemands privéleven. Allereerst wordt opgemerkt dat deze problematiek er niet één is die uitsluitend het onderzoek door inlichtingen- en veiligheidsdiensten in de publieke ruimte betreft, maar evenzeer vergelijkbaar onderzoek door andere overheidsinstanties, met name op het vlak van opsporing en vervolging van strafbare feiten. Indien ter zake al (aanvullende) regulering zou moeten worden overwogen, achten wij het noodzakelijk dat dit eerst in brede zin wordt verkend. Overigens geldt voor observaties in de publieke ruimte door inlichtingen- en veiligheidsdiensten - zie de bijzondere bevoegdheid volgen en observeren; artikel 20 Wiv 2002 en artikel 40 van het wetsvoorstel – dat deze nu reeds al zijn onderworpen aan een systeem van voorafgaande toestemming en toezicht door de CTIVD. Wij zien geen reden om die eisen te verscherpen. Daar komt bij dat de in de PIA Wiv gesignaleerde problematiek niet één is die uitsluitend aan de orde is bij observeren in de publieke ruimte, waarbij als gevolg van bijvoorbeeld het combineren van de gegevens die door de uitoefening van diverse bijzondere bevoegdheden wordt vergaard, een cumulatief beeld van iemands privéleven ontstaat.

Waar het gaat om de reikwijdte van het begrip 'geautomatiseerd werk' zoals dat in onderhavig wetsvoorstel wordt gehanteerd, wordt verwezen naar hetgeen ter zake in paragraaf 3.3.4.4.6 van de memorie van toelichting is gesteld (aanbeveling 18 Pia Wiv).

De aanbeveling om het toestemmingsvereiste voor het opvragen van verkeersgegevens op hetzelfde niveau te leggen als voor interceptie van communicatie, te weten (uitsluitend) op het niveau van de minister (aanbeveling 19) wordt niet geheel overgenomen. In de huidige Wiv 2002 is voor het opvragen in het geheel niet voorzien in een toestemmingseis, zij het dat een dergelijk verzoek uitsluitend kan worden gedaan door het hoofd van de desbetreffende dienst (artikel 28, derde en vierde lid, Wiv 2002). Ten opzichte van de huidige wet wordt in artikel 55, tweede lid, van het wetsvoorstel thans wel een toestemmingseis gesteld; de desbetreffende bevoegdheid mag slechts worden uitgeoefend met toestemming van de voor de dienst verantwoordelijke minister of namens deze het hoofd van de dienst (er is geen ondermandaat mogelijk). Naar ons oordeel kan hiermee worden volstaan. Daar komt bij dat de gegevens waarop het verzoek betrekking kan hebben bij algemene maatregel van bestuur worden aangewezen; op voorhand is dus voor de aanbieders maar ook voor de burgers waarop een dergelijk verzoek betrekking kan hebben duidelijk welke gegevens het betreft.

Het opleggen van een opdracht aan aanbieders van communicatiediensten om onderzoeksopdrachtgerichte interceptie te faciliteren is onderdeel van een zorgvuldig proces, waarbij de aanbieder van meet af aan betrokken is. In paragraaf 3.3.4.4.7.5 van de memorie van toelichting is ingegaan op de informatie- en medewerkingsplicht voor aanbieders van communicatiediensten bij de verwerving van telecommunicatie op grond van onder meer artikel 48. De daar geschetste procedure draagt naar ons oordeel bij aan het voorkomen dat de in aanbeveling 20 van de PIA Wiv gesignaleerde privacyrisico's worden gerealiseerd.

In aanbeveling 21 wordt gesteld dat onvoldoende zou zijn gemotiveerd waarom voor gerichte interceptie van militair (ook kabelgebonden) verkeer geen toestemming nodig zou zijn. Naar aanleiding hiervan hebben we alsnog voorzien in het stellen van de toestemmingseis; zie daartoe artikel 47, achtste lid, van het wetsvoorstel en paragraaf 3.3.4.4.7.3 van de memorie van toelichting.

Aanbeveling 22 ziet op de samenwerking tussen AIVD en MIVD. Daarin wordt aanbevolen om bij beantwoording van de vraag of gegevens kunnen worden verstrekt aan een collegadienst naast proportionaliteit en subsidiariteit ook doelbinding in de afweging te betrekken. Doelafwijkend gebruik door de collegadienst vergt een nieuwe grondslag en daarom ook toestemming op ten minste hetzelfde niveau als de toestemming die nodig was voor het verkrijgen van de gegevens door de verstrekkende

dienst. Allereerst wordt opgemerkt dat – anders dan in het consultatievoorstel – de verstrekking van gegevens tussen AIVD en MIVD in het kader van artikel 86 thans als een bevoegdheid is geformuleerd. Dat brengt met zich mee dat daarop de algemene bepalingen inzake gegevensverwerking van toepassing zijn (paragraaf 3.1). Dat betekent onder meer dat de verstrekking is gebonden aan een bepaald doel. Zoals eerder in de memorie van toelichting is uiteengezet impliceert de eis in artikel 18, eerste lid, van het wetsvoorstel dat de verwerking noodzakelijkheidsvereiste een toets aan proportionaliteit en subsidiariteit vergt. Aan de aanbeveling is dan ook naar ons oordeel grotendeels tegemoet gekomen. Waar het gaat om de mogelijkheid om verzamelde gegevens ook te kunnen gebruiken voor een ander doel wordt verwezen naar de uiteenzetting in paragraaf 3.3.2.3 van de toelichting. Wij zien geen aanleiding om hier aanvullend en ten opzichte van de bestaande situatie nieuw toestemmingsvereiste te introduceren gerelateerd aan de bevoegdheid waarmee de gegevens zijn verkregen.

In aanbeveling 23 wordt waar het gaat om het vragen van ondersteuning door de AIVD of MIVD *aan* een buitenlandse collegadienst aanbevolen dat de wetgever duidelijk maakt hoe geborgd kan worden dat bij het verzamelen van gegevens door buitenlandse diensten op verzoek van de Nederlandse diensten, vergelijkbare waarborgen en beperkingen in acht genomen worden als die gelden bij de uitoefening van bevoegdheden in Nederland. Allereerst wordt opgemerkt dat voorafgaand aan de vraag of een dergelijk verzoek kan worden gedaan op grond van de weging als bedoeld in artikel 88 van het wetsvoorstel wordt vastgesteld òf met een bepaalde buitenlandse dienst kan worden samengewerkt en, zo ja, wat de aard en intensiteit van de samenwerking kan zijn (artikel 88, tweede lid). Er is, met andere woorden, voorafgaand aan het doen van een verzoek om ondersteuning al het nodige voorwerk verricht. Bij een concreet verzoek om ondersteuning aan een buitenlandse dienst zal over het algemeen eerst overleg met de desbetreffende buitenlandse dienst plaatsvinden, waarbij de mogelijkheid tot ondersteuning wordt verkend. De buitenlandse dienst zal waar het gaat om de vraag of op een verzoek van de Nederlandse dienst kan worden ingegaan, immers toch ook moeten bezien of eigen wet- en regelgeving het verlenen van de gevraagde ondersteuning überhaupt mogelijk maakt en onder welke condities; dit naast andere, waaronder operationele, afwegingen. In de contacten tussen de diensten – maar ook in het uiteindelijke (formele) verzoek – dient door de Nederlandse dienst nauwkeurig aangegeven te worden waarop de te vragen ondersteuning precies ziet en ook bijvoorbeeld welke gegevens men wel of niet wil langs die weg wil verkrijgen. Het gaat echter te ver om daarbij vergelijkbare waarborgen en beperkingen te eisen als die gelden bij de uitoefening van bevoegdheden in Nederland. Dat is in het kader van internationale samenwerking niet realistisch, maar doet ook geen recht aan het feit dat elk land zijn eigen wettelijk stelsel heeft. Belangrijker is om de verschillen, onder meer

in de sfeer van waarborgen, te onderkennen en die in de besluitvorming of men een verzoek om ondersteuning wil doen nadrukkelijk te betrekken.

In aanbeveling 24 worden voor enkele artikelen verbetervoorstellen gedaan. Ter zake wordt in het kort het volgende opgemerkt.

Aan het voorstel om vanuit privacyoverwegingen een kortere bewaartermijn te hanteren voor de gegevens over informanten (en – dientengevolge ook voor – agenten) wordt geen gehoor gegeven. Om redenen uiteengezet in de toelichting op artikel 39, zesde lid, van het wetsvoorstel zien we geen aanleiding om tot verkorting van de termijn over te gaan.

Wat betreft het monitoren van sociale media wordt verwezen naar hetgeen is opgemerkt in paragraaf 3.3.4.4.2 van de memorie van toelichting.

Voor wat betreft het matchen van een DNA-profiel bij externe databanken en de daaraan (volgens de PIA Wiv) te stellen eis dat het profiel alleen voor matching, mag worden gebruikt, wordt verwezen naar paragraaf 3.3.4.4.4 van de memorie van toelichting, waar onder meer is ingegaan op de verstrekking van een DNA-profiel aan een buitenlandse diensten. Waar het gaat om de vernietiging van celmateriaal is thans in 43, vijfde lid, bepaald dat het vergaarde celmateriaal binnen drie maanden na het DNA-onderzoek dient te worden vernietigd; voor het uitvoeren van een DNA-onderzoek is in artikel 43, vierde lid, een termijn van drie maanden na vergaring van het celmateriaal gesteld (met de mogelijkheid tot eenmalige verlenging voor eenzelfde periode). Dit betekent dat uiterlijk zes maanden (dan wel negen maanden na verlenging) het celmateriaal dient te zijn vernietigd.

Waar het gaat om de aanbeveling dat voor het plaatsen van apparatuur in de woning ministeriële toestemming is vereist, wordt het volgende opgemerkt. Afhankelijk van de bevoegdheid die het betreft, is de eis van ministeriële toestemming voor de uitoefening van een bevoegdheid in woningen expliciet gesteld indien de toestemming voor de uitoefening van de bevoegdheid als zodanig ook door een ander dan de minister kan worden verleend (zie bijvoorbeeld artikel 40, derde lid, en artikel 42, vierde lid, van het wetsvoorstel). Waar de uitoefening van een bijzondere bevoegdheid altijd voorafgaande ministeriële toestemming vereist, is afgezien van het (apart) stellen van deze eis; vgl. een microfoonactie: ongeacht waar deze plaats vindt, in een woning of niet, is altijd ministeriële toestemming vereist.

Het stellen van de eis van ministeriële toestemming in alle gevallen van geautomatiseerde data-analyse wordt niet overgenomen. Dit zou leiden tot een disproportionele belasting van de operationele praktijk, zonder dat direct duidelijk is

welk probleem hiermee zou worden opgelost. Zie ook paragraaf 3.5 van de memorie van toelichting.

Tot slot wordt in aanbeveling 24 aanbevolen dat de toestemmingseis van – thans – artikel 89, vijfde en zesde lid, ook van toepassing zou moeten worden verklaard op de gegevensverstrekking als bedoeld in het eerste lid. Dat zou – afgaande op de tekst van de consultatieversie – betekenen dat de minister altijd toestemming dient te verlenen, zij het met de mogelijkheid van mandaat aan het hoofd van de dienst (zonder mogelijkheid van ondermandaat). Dat achten wij een te vergaande eis, waarbij geen rekening wordt gehouden met de dagelijkse praktijk en waarbij in de intensieve samenwerking met daarvoor in aanmerking komende diensten op diverse niveaus gegevens moeten kunnen worden uitgewisseld; uiteraard dienen daarbij wel de wettelijke voorwaarden verbonden aan de verstrekking van gegevens in acht te worden genomen. Wij menen dan ook te kunnen volstaan met de eis van ministeriële toestemming waar het gaat om de verstrekking van ongeëvalueerde gegevens.

In de aanbevelingen 25 en 26 worden met betrekking tot het wetsvoorstel nog enkele wenselijke aanvullingen of aanscherpingen voorgesteld.

Aan aanbeveling 25 is gevolg gegeven. In paragraaf 3.2.3 van de memorie van toelichting is ingegaan op het feit dat de eisen van proportionaliteit en subsidiariteit besloten liggen in de aan gegevensverwerking gestelde eisen van artikel 18.

Waar het gaat om de voorstellen onder aanbeveling 26.

Van het eisen van het opnemen van een betrouwbaarheids- of bronaanduiding van de programmatuur waarmee gegevensverzamelingen worden geanalyseerd in (thans) artikel 18, derde lid, wordt afgezien. Zie daartoe hetgeen is opgemerkt in paragraaf 3.2.3 van de memorie van toelichting. Het opnemen van het lidmaatschap van een vakvereniging als gevoelig gegeven is overgenomen. Zie daartoe artikel 19, derde lid, van het wetsvoorstel alsmede de toelichting daarop. De voorgestelde aanpassing met betrekking tot de bevoegdheid tot DNA-onderzoek (opnemen van ‘een zo nauwkeurig mogelijk aanduiding van een persoon’) is verwerkt. Het voorstel om als waarborg tegen een te omvangrijke semi-continue monitoring in het kader van het verkennen van technische kenmerken van geautomatiseerde werken die op een communicatienetwerk zijn aangesloten (artikel 45, eerste lid, onder a, van het wetsvoorstel) de eis te stellen dat bij het verzoek om toestemming ook een specificatie van de beoogde reikwijdte van het verkennen wordt opgenomen, is niet overgenomen. De formulering van artikel 54, eerste lid, van het wetsvoorstel (was 38, eerste lid) is reeds om andere redenen aangepast; zie ook de memorie van toelichting ter zake. Voor aanscherping van de eis in

het artikel inzake geautomatiseerde data-analyse, dat duidelijker is dat maatregelen niet op één of meer automatische verwerkingen mogen worden getroffen of bevorderd is naar aanleiding van het advies van de Afdeling advisering van de Raad van State is de beperking van de norm van artikel 60, derde lid, tot geautomatiseerde data-analyse aan de hand van profielen geschrapt. De opmerking met betrekking artikel 90, vijfde lid, (voorheen 78, vijfde lid) is verwerkt; de eerder opgenomen beperking is geschrapt.

Tot slot worden in de PIA nog enkele aanbevelingen (27 tot en met 29) gedaan in de sfeer van niet-wettelijke maatregelen die nodig zouden zijn voor het vinden van een goede balans tussen effectiviteit en rechtsbescherming, een en ander ter ondersteuning van de wettelijke waarborgen.

Allereerst wordt gepleit voor versterking van de capaciteit van de CTIVD (aanbeveling 27). Die versterking zou vooral ook betrekking dienen te hebben op technische expertise bij de CTIVD zelf; integratie tussen technische en juridische perspectieven is, aldus de PIA, nodig om een adequate rechtmatigheidstoets te kunnen uitoefenen. Hieromtrent wordt opgemerkt dat de CTIVD het toenemende belang van de combinatie van technologische en juridische kennis bij het toezicht eveneens gezien heeft en heeft mede daarom een kenniskring opgericht. Tevens zal zij blijven investeren in het verder professionaliseren van haar werkwijzen, waaronder het terrein van ICT-technologie, teneinde effectief toezicht te kunnen blijven uitoefenen.[310]

In aanvulling op het pleidooi voor meer capaciteit bij de CTIVD, wordt bij aanbeveling 28 – in referte aan de verzwaring van de toestemming – erop gewezen dat ook voldoende ondersteuning nodig is op het niveau van diensthoofden en ministers, om zorgvuldige afwegingen op deze niveaus te kunnen waarborgen. Niet alleen zou moeten worden voorzien in versterking van ambtelijke ondersteuning , maar ook in expertise en kritisch vermogen van degenen die verantwoordelijk zijn voor de afhandeling van toestemmingsverzoeken. Dergelijke personen zouden een opbouwend-kritische en onafhankelijke adviesfunctie moeten hebben. Hieromtrent wordt opgemerkt dat ervoor wordt zorg gedragen dat leidinggevenden en juristen van de AIVD en MIVD een goede kennis van de wettelijke regels hebben. Dit komt uitgebreid aan de orde in het opleidings- en cursusmateriaal. De CTIVD concludeert ook dat de uitoefening van de bijzondere bevoegdheden bij de diensten in het algemeen zorgvuldig en doordacht geschiedt. Tevens zij in dit kader gewezen op de kritische functie van de Directie Juridische Zaken bij het ministerie van Defensie alsmede het naar aanleiding van het rapport van de Commissie Dessens opgerichte afdeling Openbare Orde Inlichtingen en Veiligheid bij het ministerie van BZK.

[310] Jaarverslag CTIVD 2014 – 2015, p. 3. Te vinden via www.CTIVD.nl

Ten aanzien van het belang van privacybewustzijn binnen de diensten en een continue, kritische zelfreflectie op de taakopvatting en taakuitvoering (aanbeveling 29) kan het volgende opgemerkt. Hier is aandacht voor in opleiding en opfriscursussen. De rapporten van de CTIVD laten grosso modo een beeld zien van diensten (en dus ook medewerkers bij die diensten) die zorgvuldig en gewetensvol omspringen met de hen gegeven bevoegdheden.

12.4 Notificatie

Het wetsvoorstel is parallel aan de advisering door de Raad van State op grond van de Notificatierichtlijn[311] genotificeerd bij de Europese Commissie (hierna: Commissie) (notificatienummer 2016/0188/NL). Ook de huidige Wiv 2002 is indertijd genotificeerd. De notificatie heeft op 22 juli 2016 geleid tot een mededeling van de Commissie aan de Nederlandse regering, waarin enkele opmerkingen zijn gemaakt ter zake van de in het wetsvoorstel voorziene regeling betreffende de samenwerking/uitwisseling van gegevens tussen de inlichtingendiensten en ordehandhaving (lees: de met opsporing van strafbare feiten belaste instanties). Daarbij werd door de Commissie aangegeven dat de stand still-termijn (die op 22 juli 2016 afliep) door deze opmerkingen niet wordt verlengd.

De Commissie heeft in haar mededeling aangegeven dat waar het gaat om de samenwerking/uitwisseling van gegevens tussen de inlichtingen- en veiligheidsdiensten en ordehandhaving, en met name de ondersteuning door de inlichtingendiensten ten behoeve van de ordehandhaving op verzoek van deze laatste (onder artikel 93 van het wetsvoorstel; thans artikel 95), moet worden verduidelijkt welke Nederlandse bepalingen inzake de persoonsgegevens van toepassing zijn op de verwerkingsactiviteiten die vallen onder de samenwerking/uitwisseling van gegevens tussen inlichtingen- en veiligheidsdiensten en ordehandhaving.

Voorts heeft de Commissie verzocht om ervoor te zorgen dat elke gegevensverwerkingsactiviteit die wordt uitgevoerd met het oog op ordehandhaving en niet met het oog op nationale veiligheid en dus valt onder de toepassing van de politierichtlijn[312] voldoet aan alle beginselen die erin zijn vastgelegd.

De regering heeft ter zake van de door de Commissie gemaakte opmerkingen de Commissie als volgt geantwoord.

---

[311] Richtlijn (EU) 2015/1535 van het Europees Parlement en de Raad van 9 september 2015 betreffende een informatieprocedure op het gebied van technische voorschriften en regels betreffende de diensten van de informatiemaatschappij (codificatie) (PbEU 215, L241/1).

[312] Hiermee wordt bedoeld: Richtlijn (EU) 2016/680 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens en tot intrekking van Kaderbesluit 2008/977/JBZ van de Raad (PbEU 2016, L119/89).

In het wetsvoorstel wordt, evenals in de huidige Wet op de inlichtingen- en veiligheidsdiensten 2002 (Wiv 2002), voorzien in de mogelijkheid dat de Nederlandse inlichtingen- en veiligheidsdiensten en de met opsporing van strafbare feiten belaste instanties ("ordehandhaving") elkaar – onder strikte voorwaarden – ondersteuning kunnen verlenen. Het kan hierbij gaan om: (1) ondersteuning te verlenen door de inlichtingen- en veiligheidsdiensten *aan* de met opsporing van strafbare feiten belaste instanties en (2) ondersteuning te verlenen door een of meer landelijke eenheden van de politie *aan* de Nederlandse inlichtingen- en veiligheidsdiensten. In beide gevallen geldt dat er altijd een (schriftelijk) verzoek om ondersteuning voorhanden dient te zijn, waarin precies wordt omschreven welke werkzaamheden (ondersteuning) worden verlangd. De ondersteuning kan slechts worden verleend indien door of namens de verantwoordelijke minister toestemming is verleend. Indien de instantie aan wie ondersteuning wordt gevraagd instemt met het verzoek, vindt de feitelijke uitvoering van de verlangde werkzaamheden plaats onder verantwoordelijkheid van de verzoekende instantie.

Het voorgaande betekent dat indien de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) aan een landelijke eenheid van de politie om ondersteuning verzoekt en de ondersteuning wordt verleend, de verantwoordelijkheid voor de feitelijke uitvoering van de werkzaamheden waaruit de ondersteuning bestaat bij de voor de AIVD verantwoordelijke minister (in casu de minister van Binnenlandse Zaken en Koninkrijksrelaties) berust. Gegevens die aldus worden verwerkt, bijvoorbeeld gegevens uit observatiewerkzaamheden die door de politie ten behoeve van de AIVD worden verricht, zijn aan te merken als gegevens die vallen onder het regime van de Wet op de inlichtingen- en veiligheidsdiensten. Indien de AIVD op een daartoe strekkend verzoek van een met opsporing van strafbare feiten belaste instantie, zoals de politie, ondersteuning verleent, geschiedt dat onder verantwoordelijkheid van het bevoegde gezag van de desbetreffende instantie (het openbaar ministerie). Dat betekent dat als medewerkers van de AIVD ten behoeve van de politie observatiewerkzaamheden verrichten de in dat kader verwerkte gegevens zijn aan te merken als gegevens die onder het wettelijk regime voor de verwerking van gegevens door de politie vallen (in casu de Wet politiegegevens).

Tot slot is opgemerkt, dat de verwerking van gegevens met het oog op ordehandhaving (opsporing en vervolging van strafbare feiten) zal voldoen aan de beginselen die in de politierichtlijn zijn vastgelegd. Dat laat onverlet dat gegevens verwerkt door de met opsporing en vervolging van strafbare feiten belaste instanties die van belang (kunnen) zijn voor een goede taakuitvoering van de Nederlandse inlichtingen- en veiligheidsdiensten door die instanties aan die inlichtingen- en veiligheidsdiensten beschikbaar moeten worden gesteld. Zowel de huidige Wet op de inlichtingen- en

veiligheidsdiensten 2002 als het voorstel voor een nieuwe wet bevatten daartoe in het kader van de nationale veiligheid een verstrekkingsverplichting.

II Artikelsgewijze toelichting

Artikelen 8, tweede lid, onder f en artikel 10, tweede lid, onder g

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.

Artikelen 13, 14, 22 en 61

Vanwege de introductie van artikel 92 behoeven enkele andere artikelen, waarin thans al naar artikel 91 wordt verwezen, aanpassing. Voor de ambtenaren die op grond van artikel 92 worden aangewezen komen hierdoor, net als voor de ambtenaren die op grond van artikel 91 zijn aangewezen, regels omtrent het niet al dan niet mogen gebruiken van opsporingsbevoegdheden (artikel 13), reisbeperkingen (artikel 14), gegevensverwerking (artikel 22), en interne gegevensverstrekking (artikel 61) te gelden.

Artikel 21

In de in artikel 21 opgenomen regeling wordt gekozen voor een ietwat andere benadering 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, van de Archiefwet 1995 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 - overeenkomstig de bestaande regeling - 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 21, 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.

In artikel 21, tweede lid, van het wetsvoorstel 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 21, eerste lid, nog bij de diensten berusten.

Artikel 33, vierde lid

Artikel 33, vierde lid, verwijst (onder meer) naar artikel 99, eerste lid, van het wetsvoorstel, waarin de benoemingsprocedure voor de CTIVD is geregeld. Deze regeling is van overeenkomstige toepassing op de benoeming van de leden van de TIB. In deze procedure is een belangrijke rol voor de Tweede Kamer weggelegd. De Tweede Kamer doet immers per vacature een voordracht van ten minister drie personen waaruit de betrokken ministers een keuze dienen te maken. De Tweede Kamer kan hierbij de aanbeveling betrekken van een drietal kandidaten die een driemanschap van de president van de Hoge Raad, de vice-voorzitter van de Raad van State en de Nationale ombudsman op basis van de reacties op een opengestelde vacature een heeft opgesteld. Zij kan deze ook evenwel naast zich neerleggen en met een eigen kandidaat komen. De regering is bij de benoeming de leden gebonden aan de voordracht vanuit de Tweede Kamer. Mocht de regering onverhoopt zich niet kunnen vinden in de gedane voordracht, dan kan zij de Tweede Kamer verzoeken een nieuwe voordracht te doen. Na het doorlopen van een veiligheidsonderzoek en de afgifte van een verklaring van geen bezwaar kan betrokkene door de Kroon worden benoemd.

Artikel 63

In artikel 63 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.

Artikel 107

In artikel 107 is de inlichtingen- en medewerkingsplicht jegens de CTIVD uitgewerkt voor een ieder die betrokken is bij de uitvoering van de Wet op de inlichtingen- en

veiligheidsdiensten of de Wet veiligheidsonderzoeken (Wvo). Deze is naar aanleiding van het advies van de Afdeling advisering van de Raad van State uitgebreid tot een ieder die betrokken *is geweest* bij de uitvoering van de Wet op de inlichtingen- en veiligheidsdiensten en de Wet veiligheidsonderzoeken (Wvo); oud-medewerkers van de diensten zijn in die gevallen dan ook van rechtswege ontheven van hun geheimhoudingsplicht. Wel geldt ingevolge artikel 107, tweede lid, dat indien de CTIVD inlichtingen of medewerking verlangt van een persoon die betrokken is geweest bij de uitvoering van deze wet of de Wvo zij de betrokken minister voorafgaand daaraan in kennis stelt.

Artikelen 132 tot en met 134

Artikel 132 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 133 inzake de openbaarheid van de gegevens die bij de CTIVD berusten alsmede de toepasselijkheid van artikel 21 op de bij de CTIVD berustende archiefbescheiden. Voorts zijn de in artikel 23 en 24 geformuleerde zorgplichten van overeenkomstige toepassing op de CTIVD.

Artikel 143

In artikel 143, eerste lid, wordt de overtreding van de medewerkingsverplichtingen, zoals opgenomen in de artikelen 44, vijfde lid (uitleveren van brieven en andere geadresseerde zendingen), 45, twaalfde lid (meewerken aan de opdracht tot het ongedaan maken van versleuteling), 52, derde lid (verstrekken van informatie ten behoeve van toepassing artikel 47 en 48), 53, vijfde en zesde lid (uitvoeren opdracht tot interceptie ex artikel 47 en 48 resp. in stand houden technische voorzieningen), 54, vierde lid (meewerken aan opdracht tot verstrekken van opgeslagen gegevens), 55, vierde lid (meewerken aan opdracht tot verstrekken verkeersgegevens), 56, derde lid (meewerken aan opdracht verstrekken gebruikersgegevens), en 57, vierde lid (meewerken aan opdracht tot ongedaan maken 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 145

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 146 tot en met 155

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

Artikelen 157 en 158

Bij de Eerste Kamer der Staten-Generaal is thans het initiatief-wetsvoorstel voor een Wet open overheid aanhangig (Kamerstukken I, 33 328, A). Dit wetsvoorstel strekt ter vervanging van de Wet openbaarheid van bestuur (Wob). De Wob is thans niet van toepassing op de gegevens die in het kader van de Wet op de inlichtingen- en veiligheidsdiensten 2002 worden verwerkt. De Wiv 2002 kent immers een eigen regeling voor de kennisneming van gegevens die door of ten behoeve van de inlichtingen- en veiligheidsdiensten worden verwerkt. In artikel 45 van de Wiv 2002 is daartoe bepaald dat – onverminderd de kennisneming van op grond van artikel 3.3 verstrekte gegevens – van de gegevens verwerkt door of ten behoeve van een dienst slechts kennis kan worden genomen overeenkomstig de bepalingen van hoofdstuk 4 Wiv 2002. Ook waar het gaat om verstrekking van gegevens, waar paragraaf 3.3 Wiv 2002 een regeling voor geeft, geldt dat de wet een uitputtende regeling geeft (zie daartoe artikel 36, derde lid, Wiv 2002). Met het hiervoor genoemde initiatief-wetsvoorstel wordt beoogd in deze situatie geen wijziging te brengen (zie Kamerstukken II, 33 328, nr. 13, p. 23). De gekozen opzet van het initiatief-wetsvoorstel brengt echter met zich mee dat deze zich in beginsel ook uitstrekt over de informatie die bij de diensten berust, zij het dat in artikel 8.8 van dat wetsvoorstel de artikelen 3.1, 3.3., 4.1, 5.1, eerste, tweede en vijfde lid, en 5.2 niet van toepassing zijn op informatie waarvoor een bepaling geldt die is opgenomen in de bijlage bij die wet. Dat betekent onder meer dat de regeling inzake de actieve openbaarmakingsplicht en de regeling tot openbaarmaking van informatie op verzoek niet van toepassing is op die informatie waarop paragraaf 3.3, hoofdstuk 4 en artikel 81 van de Wiv 2002 van toepassing is. Daarnaast voorziet artikel 9.17 van het initiatief-wetsvoorstel in aanpassingen van de Wiv 2002 aan de tekst van de WOO.

De artikelen 157 en 158 van onderhavig wetsvoorstel voorzien in een samenloopregeling WOO en nieuwe Wiv 20.., voor het geval dat de WOO reeds in werking is getreden op

het moment dat de Wiv 20.. in werking treedt dan wel in werking treedt op een later moment dan de nieuwe Wiv. Met de inwerkingtreding van de Wiv 20.. komt de Wiv 2002 immers te vervallen en daarmee ook de in verband met de inwerkingtreding van de WOO daarin aangebrachte aanpassingen. Dat betekent dat niet alleen dient te worden voorzien in de aanpassingen in de Wiv 20.. als gevolg van de inwerkingtreding van de WOO, maar ook dat de tekst van de WOO zelf in overeenstemming dient te worden gebracht met de tekst van de nieuwe Wiv 20…

In artikel 157 wordt voorzien in de aanpassingen van de Wiv 20..; deze komen materieel gezien overeen met de wijzigingen die door de inwerkingtreding van de WOO in de huidige Wiv 2002 (zouden) zijn aangebracht. Wel is in artikel 157, onderdeel B, voorzien in een aanvulling van artikel 80 Wiv 20.., met een nieuw derde lid, waarbij de definitie van het begrip 'bestuurlijke aangelegenheid' wordt opgenomen. Een equivalent in de WOO ter zake ontbreekt. De noodzaak tot opneming van deze definitie is daarin gelegen dat in de WOO, anders dan in de Wob, het begrip bestuurlijke aangelegenheid geen rol meer speelt en daarmee ook de definitie is komen te vervallen. In de Wiv 20.. speelt dit begrip – ter afbakening van verzoeken anders dan om kennisneming van persoonsgegevens – echter nog steeds een belangrijke rol. De betekenis van het begrip 'bestuurlijke aangelegenheid' is ongewijzigd uit de Wob overgenomen in het derde lid.

In artikel 158 wordt voorzien in een tweetal aanpassingen van de WOO aan de nieuwe Wiv 20… In artikel 158, onderdeel A, wordt voorzien in een aanvulling van artikel 3.2 van de WOO, waarin de verplichting tot het bijhouden van een elektronisch toegankelijk openbaar register van bij het bestuursorgaan berustende documenten is opgenomen, met de bepaling dat deze plicht niet geldt voor documenten die bij de desbetreffende bestuursorganen berusten in verband met de uitvoering van de Wiv 20.. en de Wet veiligheidsonderzoeken. Het is evident dat documenten die verband houden met de uitvoering van genoemde wetten, zoals bijvoorbeeld verzoeken om informatieverstrekking, verzoeken om kennisneming van gegevens, door de minister uitgebrachte ambtsberichten, aanvragen voor het verrichten veiligheidsonderzoeken, uitgebrachte (weigeringen) van verklaringen van geen bezwaar, de correspondentie tussen AIVD en MIVD en met andere instanties alsmede met buitenlandse diensten, gelet op de inhoud en de veelal gerubriceerde status daarvan niet in een dergelijk openbaar register kunnen worden bijgehouden. Zeker nu dit (in)zicht biedt in de wijze waarop door de diensten, maar ook andere bij de uitvoering betrokken bestuursorganen, in het kader van de uitvoering van deze wetten wordt (samen)gewerkt. De opgenomen uitzondering ziet voor de goede orde niet alleen op documenten die bij de AIVD, MIVD, de coördinator, de CTIVD en de TIB berusten, maar ook bij andere bestuursorganen (in de zin van de WOO) die betrekking hebben op de uitvoering van de Wiv 20.. en de Wvo.

Het zal bij dit laatste in het bijzonder gaan om – al dan niet als staatsgeheim gerubriceerde – ambtsberichten die door de diensten aan die bestuursorganen zijn uitgebracht. Ambtsberichten zijn immers niet per definitie openbaar; onder omstandigheden – vgl. door de AIVD uitgebrachte ambtsberichten aan de IND – kunnen deze (mits deze net gerubriceerd zijn) door de geadresseerde bijvoorbeeld in een juridische procedure worden ingebracht.

In artikel 157, onderdeel B, wordt de bijlage bij artikel 8.8 WOO aangepast aan de tekst van de nieuwe Wiv 20… Voorts wordt deze aangevuld met enkele andere bepalingen uit de Wiv 200.. teneinde zeker te stellen dat de desbetreffende gegevens buiten de reikwijdte van de hier bedoelde bepalingen van de WOO vallen en daarop uitsluitend de in de Wiv 20.. voorziene regeling ter zake van toepassing is. De Wiv 20.. geeft immers niet alleen een uitputtende regeling voor de verwerking (waaronder begrepen de verstrekking en de kennisneming) van gegevens door of ten behoeve van de diensten, maar ook voor de gegevens bij de coördinator voor de inlichtingen- en veiligheidsdiensten, de CTIVD en de TIB. Ook de gegevens van inlichtingen- en veiligheidsdiensten die zijn opgeheven, zoals de Inlichtingendienst buitenland, vallen onder dit uitputtend (bedoelde) regime.

Artikelen 159 en 160

In artikel 159 is een samenloopregeling opgenomen in verband met de voorziene wijziging van de Rijkswet op het Nederlanderschap in het belang van de nationale veiligheid (Kamerstukken 34 356 (R2064)), waarbij tevens bij amendement van het lid van de Tweede Kamer Recourt (Kamerstukken II, 34 356 (R2064), nr. 25) is voorzien in een wijziging van artikel 64, tweede lid, van de Wiv 2002 (waarin de taak van de CTIVD limitatief is geregeld) (Artikel IA). Daarin wordt de CTIVD (tijdelijk) belast met het toezicht op de toepassing van (het in het wetsvoorstel voorgestelde) artikel 14, vierde lid, van de Rijkswet op het Nederlanderschap. Dit artikel geeft de Minister van Veiligheid en Justitie de bevoegdheid om in het belang van de nationale veiligheid het Nederlanderschap in te trekken van een persoon die de leeftijd van zestien jaar heeft bereikt en die zich buiten het Koninkrijk bevindt, indien uit zijn gedragingen blijkt dat hij zich heeft aangesloten bij een organisatie die door de minister van Veiligheid en Justitie, in overeenstemming met het gevoelen van de Rijksministerraad, is geplaatst op een lijst van organisatie die deelnemen aan een nationaal of internationaal gewapend conflict en een bedreiging vormen voor de nationale veiligheid. Artikel 159 brengt een met de voorgestelde aanvulling van artikel 64, tweede lid, Wiv 2002 overeenkomstige aanvulling van artikel 97, derde lid, van onderhavig wetsvoorstel aan, indien het voorstel tot wijziging van de Rijkswet tot wet is of wordt verheven en inwerking treedt. Met de

inwerkingtreding van onderhavig wetsvoorstel wordt immers de Wiv 2002 ingetrokken en zal de (eventueel) daarin aangebrachte (tijdelijke) taakuitbreiding van de CTIVD ook in de nieuwe Wiv 20.. dienen te worden opgenomen, zodra de Rijkswet inwerking treedt of reeds in werking is getreden.

In Artikel II, tweede lid, van het hiervoor genoemde voorstel tot wijziging van de Rijkswet wordt voorts bepaald dat de Artikelen IA en IC van de Rijkswet vijf jaren na inwerkingtreding van de Artikelen I en IB in werking treden (horizonbepaling). Dat heeft tot gevolg dat zowel de voorgestelde bevoegdheid tot het intrekken van het Nederlanderschap als het toezicht van de CTIVD daarop komt te vervallen. Artikel 160 van het wetsvoorstel voorziet erin dat vijf jaar na inwerkingtreding van de artikelen I en IB van de Rijkswet de (eventueel) in artikel 97, derde lid, van onderhavig wetsvoorstel opgenomen taak van de CTIVD als hier bedoeld, komt te vervallen.

Artikelen 161 en 162

Bij koninklijke boodschap van 8 maart 2016 is een voorstel van wet houdende regels inzake het beheer, de informatievoorziening, de controle en de verantwoording van de financiën van het Rijk, inzake het beheer van publieke liquide middelen buiten het Rijk en inzake het toezicht op het beheer van publieke liquide middelen en publieke financiële middelen (Comptabiliteitswet 2016) bij de Tweede Kamer ingediend. Dit wetsvoorstel strekt ertoe tezijnertijd de huidige Comptabiliteitswet 2001 te vervangen. In artikel 21, eerste lid, onderdeel b, van de Wiv 2002 is onder meer voorzien in de bijzondere bevoegdheid van de AIVD en MIVD tot het oprichten van rechtspersonen. Ingevolge artikel 21, achtste lid, blijft ter zake artikel 34, eerste en tweede lid, van de Comptabiliteitswet 2001 buiten toepassing (voorhangprocedure bij beide kamers der Staten-Generaal). In artikel 9.22 van voornoemd wetsvoorstel is voorzien in een aanpassing van artikel 21, achtste lid, Wiv 2002, waarbij de verwijzing naar de Comptabiliteitswet 2001 in overeenstemming wordt gebracht met de tekst van de Comptabiliteitswet 2016. In de artikelen 161 en 162 wordt voorzien in een samenloopregeling voor zowel het geval dat de nieuwe comptabiliteitswet eerder (artikel 161) als later (artikel 162) in werking treedt dan artikel 72 van onderhavig wetsvoorstel, waarin de bijzondere bevoegdheid tot het oprichten van rechtspersonen door de AIVD en MIVD is geregeld. Deze regeling strekt ertoe om de verwijzing in artikel 72, vierde lid, van onderhavig wetsvoorstel naar het desbetreffende artikel in de Comptabiliteitswet 2001 in overeenstemming te brengen met de tekst van de Comptabiliteitswet 2016.

Artikel 163

Bij koninklijke boodschap van 19 januari 2016 is het voorstel van wet houdende regels over het verwerken van gegevens ter bevordering van de veiligheid en de integriteit van elektronische informatiesystemen die van vitaal belang zijn voor de Nederlandse samenleving en regels over het melden van ernstige inbreuken (Wet gegevensverwerking en meldplicht cybersecurity) (Kamerstukken 34 388) bij de Tweede Kamer der Staten-Generaal ingediend. In artikel 9, tweede lid, onderdeel b, van dat wetsvoorstel wordt verwezen naar de inlichtingen- en veiligheidsdiensten, bedoeld in de Wet op de inlichtingen- en veiligheidsdiensten 2002. Artikel 163 van onderhavig wetsvoorstel strekt ertoe de desbetreffende verwijzing naar de huidige wet in overeenstemming te brengen met de nieuwe wet ingeval dat wetsvoorstel tot wet is of wordt verheven.

Artikel 164

Bij koninklijke boodschap van 12 september 2016 is het voorstel van wet tot wijziging van de Telecommunicatiewet en het Wetboek van Strafvordering in verband met de bewaring van gegevens die zijn verwerkt in verband met het aanbieden van openbare telecommunicatiediensten en openbare telecommunicatienetwerken (aanpassing bewaarplicht telecommunicatiegegevens)(Kamerstukken 34 537) bij de Tweede Kamer ingediend. Daarin wordt voorzien in een herformulering van de artikelen 13.4 en 13.5 van de Telecommunicatiewet. De daarin opgenomen verwijzingen naar bepalingen uit de huidige wet dienen te worden aangepast aan de tekst van de nieuwe wet op het moment dat dat wetsvoorstel tot wet is of wordt verheven.

Artikel 165

In dit artikel 165 wordt – conform het bepaalde in artikel 99 Wiv 2002 - de in artikel 59 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 166

In artikel 88 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 88, tweede lid, dienen plaats te vinden, waarbij in ieder geval de in het derde lid opgenomen criteria dienen te worden toegepast. Indien er risico's blijken te bestaan aan de samenwerking dient ingevolge het vierde lid de voor de dienst verantwoordelijke minister toestemming te geven. Een weging dient opnieuw plaats te vinden indien omstandigheden daartoe aanleiding geven (vijfde lid). In de artikelen 89, zesde lid, en 90, 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 88 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 166 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 167

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.[313] 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 167 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 169

Artikel 169 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.

[313] Rapport van de commissie Dessens, *Evaluatie Wet op de inlichtingen- en veiligheidsdiensten 2002. Naar een nieuwe balans tussen bevoegdheden en waarborgen*, par. 8.4 (blz. 171).

Er zal naar gestreefd worden de aangepaste besluiten gelijktijdig met de nieuwe wet in werking te laten treden.

Artikel 170

De commissie van toezicht op de inlichtingen- en veiligheidsdiensten (CTIVD) wordt in onderhavig wetsvoorstel op een andere wijze gestructureerd. De commissie komt niet alleen te bestaan uit vier leden, waaronder de voorzitter, maar tevens worden er twee afdelingen in het leven geroepen; de afdeling toezicht en de afdeling klachtbehandeling. Om onduidelijkheid te voorkomen inzake de positie van de bestaande leden van de CTIVD wordt in artikel 170 een overgangsrechtelijke voorziening getroffen. Deze strekt ertoe dat de huidige leden van de CTIVD na inwerkingtreding van deze wet lid blijven van de commissie van toezicht. Het lidmaatschap van de commissie van toezicht – ook qua (resterende) benoemingsduur – wordt dus onder deze wet gecontinueerd. Aangezien in onderhavig wetsvoorstel ook wordt voorzien in de instelling van een afdeling klachtbehandeling, die in staat moet zijn om van meet af aan klachten in behandeling te kunnen nemen, is er tevens in voorzien dat de commissie uit haar midden een voorzitter van de afdeling klachtbehandeling aanwijst. De andere twee leden zijn lid van de afdeling toezicht.

Voor het personeel van de CTIVD is een dergelijke overgangsrechtelijke voorziening niet vereist. Zij zijn en blijven in dienst van de CTIVD.

Artikel 171, eerste lid

De Wet raadgevend referendum (Wrr) is van toepassing op onderhavig wetsvoorstel, indien dat tot wet is verheven. Normaliter brengt dat met zich mee dat het tijdstip voor inwerkingtreding niet eerder kan worden gesteld dan acht weken na de mededeling in de Staatscourant van het besluit dat over de wet een referendum kan worden gehouden (deze mededeling wordt binnen een week na bekrachtiging van de wet gepubliceerd). Voor spoedeisende, referendabele wetten biedt de Wrr een afwijkingsmogelijkheid. Artikel 12, eerste lid, bepaalt dat de inwerkingtreding afwijkend kan worden geregeld als de inwerkingtreding van een wet geen uitstel kan lijden. Dat betekent echter niet dat er dan geen raadgevend referendum kan worden gehouden; dat blijft mogelijk. Naar het oordeel van de regering dient onderhavig wetsvoorstel, zodra zij tot wet is verheven zo spoedig mogelijk in werking te treden en dient aldus toepassing te worden gegeven aan artikel 12 Wrr. Artikel 171, eerste lid, van het wetsvoorstel voorziet daarin.

De dreiging van terrorisme is in Nederland groter dan ooit. In de ons omringende landen vinden geregeld dodelijke aanslagen plaats. Daarnaast nemen cyberaanvallen en onrust aan de grenzen van Europa toe. Informatie over plannen en het werk van terroristen,

statelijke actoren en andere kwaadwillenden blijft deels en soms volledig uit het zicht van de diensten vanwege beperkingen in hun onderzoeksmogelijkheden als gevolg van een op onderdelen sterk verouderde Wiv 2002. De diensten worden hierdoor ernstig belemmerd in hun taakuitvoering ten behoeve van de nationale veiligheid. Gelet hierop is het noodzakelijk dat de nieuwe wet, na plaatsing in het Staatsblad, onmiddellijk in werking treedt. De inwerkingtreding van de nieuwe wet kan niet wachten op het tijdstip waarop vast komt te staan dat er geen referendum zal worden gehouden of op de uitslag van een eventueel referendum en de daaraan verbonden gevolgen.

De Minister-President, Minister van Algemene Zaken,

De Minister van Binnenlandse Zaken en Koninkrijksrelaties,

De Minister van Defensie,

De Minister van Veiligheid en Justitie,

Bijlage 1

Transponeringstabel

Artikel wetsvoorstel	Artikel wetsvoorstel Raad van State versie	Artikel concept-wetsvoorstel (consultatie-versie)	Artikel Wiv 2002	Omschrijving
1	1	1	1	Definitiebepaling
2	2	2	2	Gebondenheid aan de wet en ondergeschikt aan de betrokken minister
3	3	3	3	Overleg betrokken ministers
4	4	4	4	Coördinator IVD
5	5	5		Instelling en taak CVIN
6	6	6		Vaststelling geïntegreerde aanwijzing (GA)
7	7	7	5	Informatieplicht jegens coördinator
8	8	8	6	Instelling en taak AIVD
9	9	9	6a	Informatie tbv dreigings- en risicoanalyses BB
10	10	10	7	Instelling en taak MIVD
11	11	11	7a	Informatie tbv dreigings- en risicoanalyses BB
12	12	12	8	Jaarverslag diensten
13	13	13	9	Geen bevoegdheid opsporing strafbare feiten
14	14	14	10	Verblijfs- en reisverbod risicolanden
15	15	15		Zorgplicht hoofden van dienst voor beveiliging medewerkers
16	16	16	11	Bevoegdheid nadere regelstelling organisatie, werkwijze en beheer diensten
17	17	17	12, eerste lid	Algemene bevoegdheid gegevensverwerking
18	18	17	12, tweede tot en met vierde lid	Algemene eisen gegevensverwerking (doelbinding, noodzakelijkheid, overeenstemming met de wet, behoorlijke en zorgvuldige wijze, betrouwbaarheids- c.q. bronaanduiding)
19	19	18	13	Verwerking persoonsgegevens
20	20	57	43	Verwijdering, vernietiging en verbetering gegevens
21	21	58	44	Afwijking Archiefwet 1995 inzake overbrenging archiefbescheiden
22	22	19	14	Van toepassingverklaring 17, 18 en 19 op "RID-en" (artikel 91 en 92), scheiding gegevensverwerking en verantwoordelijkheid archieven
23	23	20	15	Zorgplicht diensthoofden geheimhouding gegevens, bronnen en veiligheid bronnen
24	24	21	16	Zorgplicht diensthoofden voor voorzieningen mbt zorgvuldige gegevensverwerking
25	25			Aanduiding bronnen waaruit diensten bevoegd zijn gegevens te verzamelen
26	26	43 en 44	31 en 32	Proportionaliteits- en subsidiariteitstoets; staken bevoegdheden bij bereiken doel c.q. inzet minder ingrijpende bevoegdheid
27	27			Verplichting tot toetsen van gegevens op relevantie; bewaartermijn; vernietigingsplicht
28	28	23	18	Reikwijdte toepassing bijzondere bevoegdheden
29	29	24	19	Toestemmingsduur en eisen aan verzoek om toestemming
30				Toestemmingverlening in bijzondere gevallen
31	30	45	33	Aantekening houden inzet bijzondere bevoegdheid
32	31			Instelling en taakstelling Toetsingscommissie inzet bevoegdheden (TIB)
33	32			Samenstelling TIB, eisen aan lid en plv. leden, verbod op lidmaatschap CTIVD of afdeling klachtbehandeling CTIVD, overeenkomstige toepassing benoemingsprocedure CTIVD
34	33			Secretariaat TIB
35	34			Reglement van orde TIB, vergaderingen niet openbaar,

				van overeenkomstige toepassing zorgplichten en gegevens die in het kader van de taakuitvoering aan de TIB zijn verstrekt zijn niet openbaar
36	35			Verplichting minister om aangewezen toestemmingen ter toetsing voor te leggen aan de TIB, opschorting uitoefening bevoegdheid in afwachting oordeel TIB, zelfstandige oordeelsbevoegdheid lid en plv. leden TIB, gemotiveerd onrechtmatigheidsoordeel TIB met van rechtswege vervallen van verleende toestemming
37	36			Spoedprocedure
38	37			Stelselmatig verzamelen van gegevens omtrent personen uit open bronnen, toestemmingsregeling ex artikel 29 van overeenkomstige toepassing
39	38	22	17	Raadpleging van informanten
40	39	25	20	Volgen en observeren
41	40	26	21	Inzet agenten
42	41	27	22	Onderzoek van besloten plaatsen, van gesloten voorwerpen, aan voorwerpen en DNA-onderzoek
43	42	28		DNA-onderzoek
44	43	29	23	Openen van brieven en andere geadresseerde zendingen
45	44	30	24	Verkennen van en binnendringen in geautomatiseerde werken
46	45	31		Definitiebepalingen in het kader van onderzoek van communicatie (aanbieder van een communicatiedienst, gebruiker van een communicatiedienst)
47	46	32	25	Met technisch hulpmiddel gericht aftappen e.d.
48	47	33	(deels) 27	Met technisch hulpmiddel onderzoeksopdrachtgericht aftappen e.d. van telecommunicatie of gegevensoverdracht d.m.v. geautomatiseerd werk
49	48	34	(deels) 26	Onderzoek aan ingevolge artikel 48 geïntercepteerde communicatie
50	49	35	(deels) 27	Selectie en metadata-analyse m.b.t. ingevolge artikel 48 geïntercepteerde communicatie
51	50			Toepassingsbereik artikelen 52 en 53
52	51	36		Bevoegdheid informatie-inwinning bij resp. informatieplicht van aanbieders van communicatiediensten i.v.m. toepassing artikel 47 en 48; kostenregeling
53	52	37		Bevoegdheid inroepen van en plicht tot medewerking aanbieders van communicatiediensten i.v.m. toepassing artikel 47 en 48; kostenregeling
54	53	38		Opvragen opgeslagen gegevens
55	54	39	28	Opvragen verkeersgegevens
56	55	40	29	Opvragen abonneegegevens
57	56	41		Medewerkingsplicht ontsleuteling communicatie
58	57	42	30	Toegang tot plaatsen
59	58	46	34	Notificatieplicht
60	59	47		Geautomatiseerde data-analyse
61	60	48	35	Regeling interne verstrekking (need to know)
62	61	49	36	Bevoegdheid verstrekking gegevens i.h.k.v. goede taakuitvoering
63	62	50		Gegevensverstrekking bij verzoek om naslag
64				Verstrekking ongeëvalueerde gegevens in het kader van de goede taakuitvoering aan buitenlandse diensten
65	63	51	37	Voorwaarden aan verder gebruik verstrekte gegevens (w.o. derde partij-regel)
66	64	52	38	Verstrekking gegevens aan met opsporing en vervolging van strafbare feiten belaste instanties, recht op inzage LOvJ in onderliggende gegevens
67	65	53	39	Verstrekking ingeval van dringende en gewichtige redenen anders dan i.h.k.v. een goede taakuitvoering, discretionaire bevoegdheid tot inzageverlening aan desbetreffende instantie in onderliggende gegevens
68	66	54	40	Schriftelijke mededeling persoonsgegevens aan instanties die daarop kunnen acteren jegens betrokkene, discretionaire bevoegdheid tot inzageverlening aan desbetreffende instantie in onderliggende gegevens
69	67	55	41	Verstrekking van gegevens waarvan de juistheid redelijkerwijs niet kan worden vastgesteld of ouder zijn

				dan 10 jaar
70	68	56	42	Aantekening houden van verstrekking persoonsgegevens
71	69	59		Van overeenkomstige toepassing verklaring artikelen 28, 29 en 31 bij inzet overige bijzondere bevoegdheden (geen gegevensverwerking)
72	70	60	(deels) 21	Oprichten en inzet rechtspersonen
73	71	61	(deels) 21	Bevorderen of treffen van maatregelen
74	72	62	45	Bepaling inzake gesloten inzagestelsel
75	73	63	46	Definitiebepaling
76	74	64	47	Aanvraag, behandelingstermijn en inzage eigen persoonsgegevens
77	75	65	48	Afleggen schriftelijke verklaring nav inzage eigen persoonsgegevens
78	76	66	49	Inzage door (oud) medewerkers van de dienst in hem betreffende gegevens in de personeels- en salarisadministratie
79	77	67	50	Aanvraag inzage persoonsgegevens van overleden familieleden (eerste graads)
80	78	68	51	Aanvraag, behandelingstermijn en inzage andere gegevens dan persoonsgegevens (bestuurlijke aangelegenheid)
81	79	69	52	Regeling inzake wijze van kennisneming gegevens
82	80	70	53	Weigeringsgrond eigen persoonsgegevens ivm actueel kennisniveau
83	81	71	54	Weigeringsgrond persoonsgegevens overleden familieleden ivm actueel kennisniveau
84	82	72	55	Absolute en relatieve weigeringsgronden; informatieplicht jegens CTIVD bij weigering inzage
85	83	73	56	Beperkingsgronden
86	84	74	58	Samenwerking AIVD en MIVD
87	85	75		Informatieplicht over en weer AIVD en MIVD inzake operationele activiteiten (deconflictie)
88	86	76	59, eerste lid	Samenwerking met buitenlandse diensten; afwegingskader; toestemmingsregeling
89	87	77	59, tweede tot en met zesde lid	Verstrekking van gegevens en verlenen van technische en andere vormen van ondersteuning aan buitenlandse diensten
90	88	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
91	89	79	60	Inzet medewerkers andere instanties onder verantwoordelijkheid min BZK en op aanwijzing hoofd AIVD
92	90	80		Inzet medewerkers Kmar onder verantwoordelijkheid min Def en op aanwijzing hoofd MIVD
93	91	81	61	Informatieverplichting openbaar ministerie; overlegregeling diensten – openbaar ministerie
94	92	82	62	Informatieverplichting ambtenaren politie, KMar en rijksbelastingdienst
95	93	83	63	Technische en andere vormen van ondersteuning (over en weer) diensten – politie/KMar
96	94	84		Grondslag voor nadere regelstelling inzake samenwerkingsverbanden diensten en andere instanties
97	95	85[314]	64	Instelling en taak CTIVD, afdeling toezicht en afdeling klachtbehandeling
98	96	86	65, eerste en tweede lid	Samenstelling en benoeming leden CTIVD en afdelingen
99	97	87	65, tweede tot en met achtste lid	Benoemingsprocedure en vereisten leden
100	98	88	66	Ontslagregeling leden
101	99	89	67	Regeling non actiefstelling

[314] 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.

102	100	90	68	Grondslag regeling rechtspositie leden
103	101	91	69	Regeling inzake ondersteuning door secretariaat
104	102	92	70	Overeenkomstige toepassing verblijf- en reisverboden ex artikel 14; ontheffingsbevoegdheid bij minister-president
105	103	93	71	Reglement van orde afdelingen CTIVD
106	104	94	72	Vergaderingen CTIVD en haar afdelingen zijn niet openbaar
107	105	95	73	Informatie- en medewerkingsplicht betrokkenen bij uitvoering Wiv en Wvo
108	106	96	74	Bevoegdheid afdelingen CTIVD oproepen getuigen en deskundigen
109	107	97	75	Afleggen een of belofte getuigen; verplichting onpartijdige taakuitvoering deskundige
110	108	98	76	Bevoegdheid afdelingen CTIVD om bepaalde werkzaamheden aan deskundigen op te dragen
111	109	99	77	Binnentredingsbevoegdheid afdelingen CTIVD (m.u.v. woningen)
112	110	100	78	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
113	111	101	79	Procedure toezichtsrapport
		102 **(vervallen)**		Heroverwegingsregeling m.b.t. verleende toestemming uitoefening desbetreffende bijzondere bevoegdheden; plicht heroverweging minister en informeren van TK bij afwijking van oordeel afdeling toezicht CTIVD
114	112	103	83	Indiening klacht bij afdeling klachtbehandeling; kenbaarheidsvereiste; titel 9.2 Awb n.v.t.; Nationale ombudsman onbevoegd
115	113	104		Inhoud klaagschrift
116	114	105		Verschoningsregeling medewerken aan behandeling klaagschrift
117	115	106		Hoor en wederhoor (klager/bestuursorgaan)
118	116	107		Behandeling van de klacht (samenstelling); plicht in behandeling nemen klacht (tenzij); toepasselijkheid hoofdstuk 2 Awb
119	117	108		Doorverwijzingsregeling (indien mogelijkheid van bezwaar, beroep of beklag openstaat)
120	118	109		Onbevoegdheid instellen of voortzetten behandeling klacht
121	119	110		Niet verplicht instellen of voortzetten klachtbehandeling
122	120	111		Niet verplicht instellen of voortzetten klachtbehandeling na bepaald tijdsverloop (een jaar)
123	121	112		Mededeling aan klager of bestuursorgaan indien geen onderzoek ingesteld of voortgezet
124	122	113		Beoordeling klacht (behoorlijk); verbinden gevolgen aan oordeel; informeren klager en minister; verplichting minister opvolging oordeel
125	123	114		Definitiebepaling bij regeling behandeling van meldingen inzake vermoedens van misstanden
126	124	115		Bevoegdheid melden vermoeden van misstand bij afdeling klachtbehandeling; inhoud melding
127	125	116		In behandeling nemen melding; informeren minister; bescherming identiteit melder
128	126	117		Niet verplicht instellen of voortzetten onderzoek
129	127	118		Mededeling aan melder en minister ingeval niet instellen of voorzetten onderzoek naar melding misstand
130	128	119		Hoor en wederhoor bij onderzoek melding
131	129	120		Onderzoek melding; opstellen rapport; voorleggen concept aan minister voor reactie; vaststelling rapport; verdere procedure en gevolgen oordeel of aanbeveling
132	130	121	80	Jaarverslag CTIVD
133	131	122	81	Gegevens die in het kader van de taakuitvoering aan de CTIVD en haar afdelingen zijn verstrekt zijn niet openbaar
134	132	123	82	Van overeenkomstige toepassing verklaring artikel 23 en 24 op CTIVD

135	133	124	85	Geheimhoudingsplicht
136	134	125	86	Uitzondering geheimhoudingsplicht; verschoningsplicht indien opgeroepen als getuige of deskundige, tenzij er een ontheffing is verleend
137	135	126	87	Geheimhouding inlichtingen en stukken in bestuursrechtelijke procedures
138	136	127		Geheimhouding inlichtingen en stukken in civielrechtelijke procedures
139	137	128	88	Beslissing geheimhouding stukken ingeval van inschakeling adviescommissie ex 7:13 Awb voorbehouden aan minister
140	138	129	88a	Wiv van toepassing op de BES
141	139	130	88b	Voor toepassing Wiv is Algemene wet op het binnentreden van toepassing op de BES
142	140	131	88c	Medewerkingsverplichting telecomaanbieders BES bij uitvoering bevoegdheden inzake onderzoek van telecommunicatie
143	141	132	89	Strafbaarstelling niet voldoen aan informatie- en medewerkingsverplichtingen
144	142	133	90	Toepasselijkheid diverse bepalingen op gegevensverwerking door of ten behoeve inlichtingen- en veiligheidsdiensten die zijn opgeheven
145	143	134	91	Buiten toepassing verklaring van de Awb en bestuursrecht BES op operationele besluiten IVD
146	144	135		Aanpassing Telecommunicatiewet
147	145	136		Aanpassing Aanpassingswet invoering bachelor-masterstructuur
148	146	137		Aanpassing Algemene wet bestuursrecht
149	147	138		Aanpassing Wet Incompatibiliteiten Staten-Generaal en Europees Parlement
150	148	139		Aanpassing Wet politiegegevens
151	149	140		Aanpassing Wetboek van Strafrecht
152	150	141		Aanpassing Ambtenarenwet
153	151	142		Aanpassing Vreemdelingenwet 2000
154	152	143		Aanpassing Wet bescherming persoonsgegevens
155	153	144		Aanpassing Wet bevordering integriteitsbeoordelingen door het openbaar bestuur
156				Aanpassing Wet huis voor klokkenluiders
157				Samenloopbepaling in verband met voorstel van wet open overheid
158				Samenloopbepaling in verband met voorstel van wet open overheid
159				Samenloopbepaling in verband met voorstel van Rijkswet tot wijziging Rijkswet Nederlanderschap
160				Samenloopbepaling in verband met voorstel van Rijkswet tot wijziging Rijkswet Nederlanderschap
161				Samenloopbepaling in verband met voorstel voor een Comptabiliteitswet 2016
162				Samenloopbepaling in verband met voorstel voor een Comptabiliteitswet 2016
163				Samenloopbepaling in verband met voorstel van wet gegevensverwerking en meldplicht cybersecurity
164				Samenloopbepaling in verband met voorstel van wet gegevensverwerking en meldplicht cybersecurity
165	154	145	99	Uitzonderen notificatieplicht voor bijzondere bevoegdheden ingezet voor inwerkingtreding Wiv 2002
166	155	146		Tijdelijk buiten toepassingverklaring regeling inzake weging en toestemming samenwerking met buitenlandse diensten voor bestaande samenwerkingsrelaties
167	156	147		Evaluatiebepaling
168	157	148		Intrekking Wiv 2002
169	158	149		Nieuwe grondslag uitvoeringsregelingen
170				Overgangsrechtelijke voorzieningen huidige leden CTIVD
171	159	150		Inwerkingtredingartikel en vaststellen nieuwe nummering
172	160	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 bepalingen

Paragraaf 3.2.2. Toetsingscommissie inzet bevoegdheden

Paragraaf 3.2.2.1. De instelling, taakstelling, samenstelling en andere bijzondere bepalingen met betrekking tot de toetsingscommissie

Paragraaf 3.2.2.2. De toetsing door de toetsingscommissie

Paragraaf 3.2.3. Stelselmatig verzamelen van gegevens omtrent personen uit open bronnen

Paragraaf 3.2.4. Raadpleging van informanten

Paragraaf 3.2.5. Bijzondere bevoegdheden van de diensten

Paragraaf 3.2.5.1. Observeren en volgen

Paragraaf 3.2.5.2. Agenten

Paragraaf 3.2.5.3. Onderzoek van besloten plaatsen, van gesloten voorwerpen en DNA-onderzoek

Paragraaf 3.2.5.4. Openen van brieven en andere geadresseerde zendingen

Paragraaf 3.2.5.5. Verkennen van en binnendringen in geautomatiseerde werken

Paragraaf 3.2.5.6. Onderzoek van communicatie

Paragraaf 3.2.5.6.1. Algemeen

Paragraaf 3.2.5.6.2. Onderzoek van communicatie met betrekking tot specifieke personen, organisaties en nummers dan wel technische kenmerken

Paragraaf 3.2.5.6.3. Onderzoeksopdrachtgericht onderzoek van communicatie

Paragraaf 3.2.5.6.4. Informatie- en medewerkingsplicht aanbieders van communicatiediensten bij de verwerving van telecommunicatie op grond van artikel 47 en 48

Bijlage 3 Overzicht bijzondere bevoegdheden en waarborgen

Bijzondere bevoegdheid[315][316]	**Instantie die toestemming verleent**	**Duur**	**Toets**	**Bewaartermijn c.q. vernietigingstermijn gegevens**	**Functiescheiding/ taakscheiding/ compartimentering**
Observeren en volgen (artikel 40)	Minister of hoofd dienst; ondermandaat mogelijk. Minister en toets TIB indien inzet technische hulpmiddelen in woningen betreft.	Max. 3 maanden; verlenging voor eenzelfde periode mogelijk (artikel 29, eerste lid)	Doel, noodzakelijkheid, proportionaliteit, subsidiariteit.	Een jaar, met eenmalige verlengingsmogelijkheid van zes maanden (artikel 27, eerste en derde lid)	Niet van toepassing
Agenten (artikel 41)	Minister of hoofd van dienst; ondermandaat mogelijk	Max. een jaar; verlenging voor eenzelfde periode mogelijk.	Doel; noodzakelijkheid; proportionaliteit; subsidiariteit.	Een jaar, met eenmalige verlengingsmogelijkheid van zes maanden (artikel 27, eerste en derde lid)	Niet van toepassing.
Doorzoeken besloten plaatsen; doorzoeken gesloten voorwerpen; verrichten van onderzoek aan een voorwerp gericht op vaststellen identiteit (artikel 42)	Minister of hoofd dienst; ondermandaat mogelijk. Minister en toets TIB indien het doorzoeken van woningen betreft.	Max. 3 maanden; verlenging voor eenzelfde periode mogelijk (artikel 29, eerste lid)	Doel; noodzakelijkheid; proportionaliteit; subsidiariteit.	Een jaar, met eenmalige verlengingsmogelijkheid van zes maanden (artikel 27, eerste en derde lid).	Niet van toepassing.
DNA-onderzoek gericht op vaststellen (inclusief verificatie) identiteit (artikel 43)	Minister en toets TIB, ook waar het gaat om verdere verwerking van resultaten DNA-onderzoek.	Max. 3 maanden; verlenging voor eenzelfde periode mogelijk, na toestemming van minister en TIB. Naar zijn aard echter geldig voor een specifiek onderzoek.	Doel; noodzakelijkheid; proportionaliteit; subsidiariteit.	DNA-onderzoek dient binnen drie maanden na vergaring celmateriaal te worden uitgevoerd met eenmalige verlengingsmogelijkheid indien het onderzoek binnen de eerste termijn niet kan worden uitgevoerd. Celmateriaal dient te worden vernietigd indien binnen drie maanden na vergaring geen DNA-onderzoek heeft plaatsgevonden, tenzij sprake is van verlenging met maximaal drie maanden. Daarna binnen drie maanden na DNA-onderzoek vernietigen. Maximale bewaartermijn celmateriaal is in totaal 9 maanden. DNA-profielen mogen max. 5 jaar worden bewaard; verlenging mogelijk met toestemming minister, zij het dat de totale bewaartermijn niet meer dan 30 jaar mag bedragen.	Toegang tot de gegevens wordt bij algemene maatregel van bestuur ingekaderd.
Openen van brieven en andere geadresseerde zendingen (artikel 44)	Rechtbank Den Haag	Voor een brief of andere geadresseerde zending in bezit van de dienst: per brief of geadresseerde zending. In overige gevallen: max. 3 maanden; verlenging voor eenzelfde periode mogelijk.	Doel; noodzakelijkheid; proportionaliteit; subsidiariteit.	Een jaar, met eenmalige verlengingsmogelijkheid van zes maanden (artikel 27, eerste en derde lid)	Niet van toepassing.

[315] Voor zover uitoefening plaatsvindt jegens een journalist of een advocaat, waarbij de uitoefening is gericht op het achterhalen van de bron van de journalist, is toestemming van de rechtbank Den Haag vereist.
[316] 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. (artikel 24, vijfde lid).

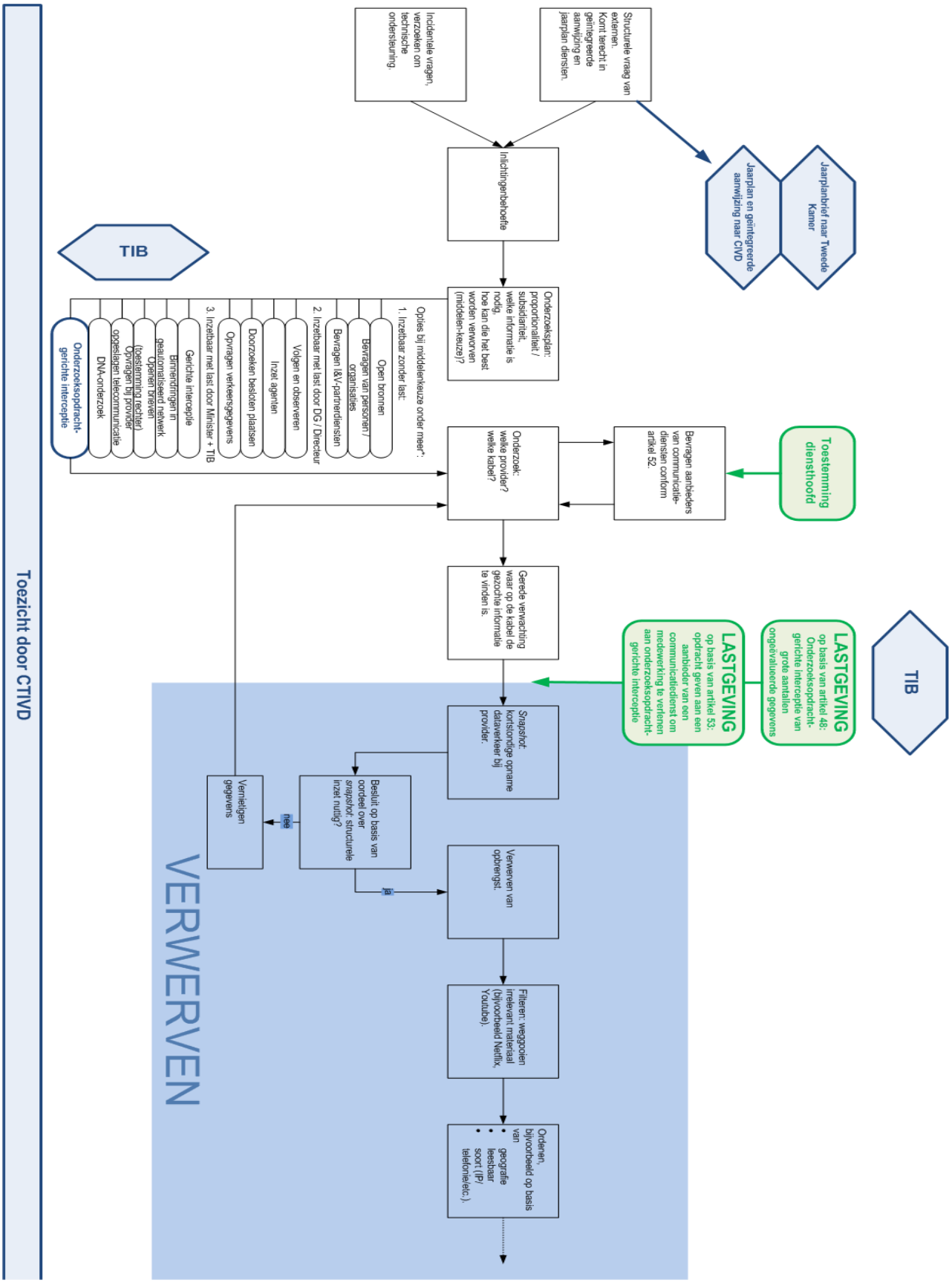
Verkennen en binnendringen van geautomatiseerde werken; medewerkingsplicht derden bij ontsleuteling (artikel 45)	Minister en toets TIB; ook waar het gaat om de medewerkingsplicht bij ontsleuteling.	Max. 3 maanden; verlenging voor eenzelfde periode mogelijk.	Doel; noodzakelijkheid; proportionaliteit; subsidiariteit.	Een jaar, met eenmalige verlengingsmogelijkheid van zes maanden (artikel 27, eerste en derde lid)	Het hoofd van de dienst wijst aan hem ondergeschikte ambtenaren aan die bij uitsluiting van anderen zijn belast met de feitelijke uitvoering van de bevoegdheid (artikel 45, zesde lid)
Onderzoek van communicatie m.b.t. specifieke personen, organisaties en nummers dan wel technische kenmerken (artikel 47)	Minister en toets TIB (ook bij binnendringen van geautomatiseerd werk van een derde en bij opdracht tot medewerking aan persoon bij ontsleuteling). Bij militair verkeer toestemming hoofd van de MIVD, tenzij medewerking aanbieder van communicatiedienst is vereist (dan toestemming minister).	Max. 3 maanden; verlenging voor eenzelfde periode mogelijk.	Doel; noodzakelijkheid; proportionaliteit; subsidiariteit.	Een jaar, met eenmalige verlengingsmogelijkheid van zes maanden (artikel 27, eerste en derde lid) Ingeval van toepassing bevoegdheid m.b.t. militair verkeer dient niet-militair verkeer terstond te worden vernietigd.	Niet van toepassing.
Onderzoeksopdrachtgerichte interceptie (artikel 48)	Minister en toets TIB.	Max. een jaar; verlenging voor eenzelfde periode mogelijk.	Doel; noodzakelijkheid; proportionaliteit; subsidiariteit.	Verkregen gegevens mogen voor een periode van ten hoogste drie jaren worden bewaard t.b.v. een verwerking als bedoeld in artikel 49 en 50; niet-relevante of niet op relevantie onderzochte gegevens worden daarna vernietigd. (artikel 48, vijfde lid)	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.
Onderzoek aan gegevens verworven o.g.v. artikel 48: search gericht op interceptie en search gericht op selectie (artikel 49)	Minister en toets TIB.	Max. een jaar; verlenging voor eenzelfde periode mogelijk.	Doel; noodzakelijkheid; proportionaliteit; subsidiariteit.	Zie regeling bij artikel 48.	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 (artikel 50, eerste lid, onder a); metadata-analyse (artikel 50, eerste lid, onder b)	Minister en toets TIB voor selectie van gegevens; minister en toets TIB 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 48.	Niet van toepassing.
Informatieplicht aanbieder van communicatiediensten i.v.m. toepassing artikel 47 en 48 (artikel 52)[317]	Geen toestemming vereist. Opdracht aan aanbieder geschiedt door hoofd van de dienst.	Niet van toepassing.	Doel; noodzakelijkheid; proportionaliteit; subsidiariteit.	Een jaar, met eenmalige verlengingsmogelijkheid van zes maanden (artikel 27, eerste en derde lid)	Niet van toepassing.
Medewerkingsplicht aanbieder van communicatiediensten bij uitvoering verleende toestemming ex artikel 47, tweede lid, 48, tweede lid (artikel 53)[318]	Minister en toets TIB.	Max. 3 maanden t.a.v. bevoegdheid onder artikel 47 en 12 maanden t.a.v. bevoegdheid onder artikel 48; 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 54)	Minister en toets TIB.	Max. 3 maanden; verlenging voor eenzelfde periode mogelijk.	Doel; noodzakelijkheid; proportionaliteit; subsidiariteit.	Een jaar, met eenmalige verlengingsmogelijkheid van zes maanden (artikel 27, eerste en derde lid)	Niet van toepassing.

[317] Ondersteunende bevoegdheid.
[318] Ondersteunende bevoegdheid.

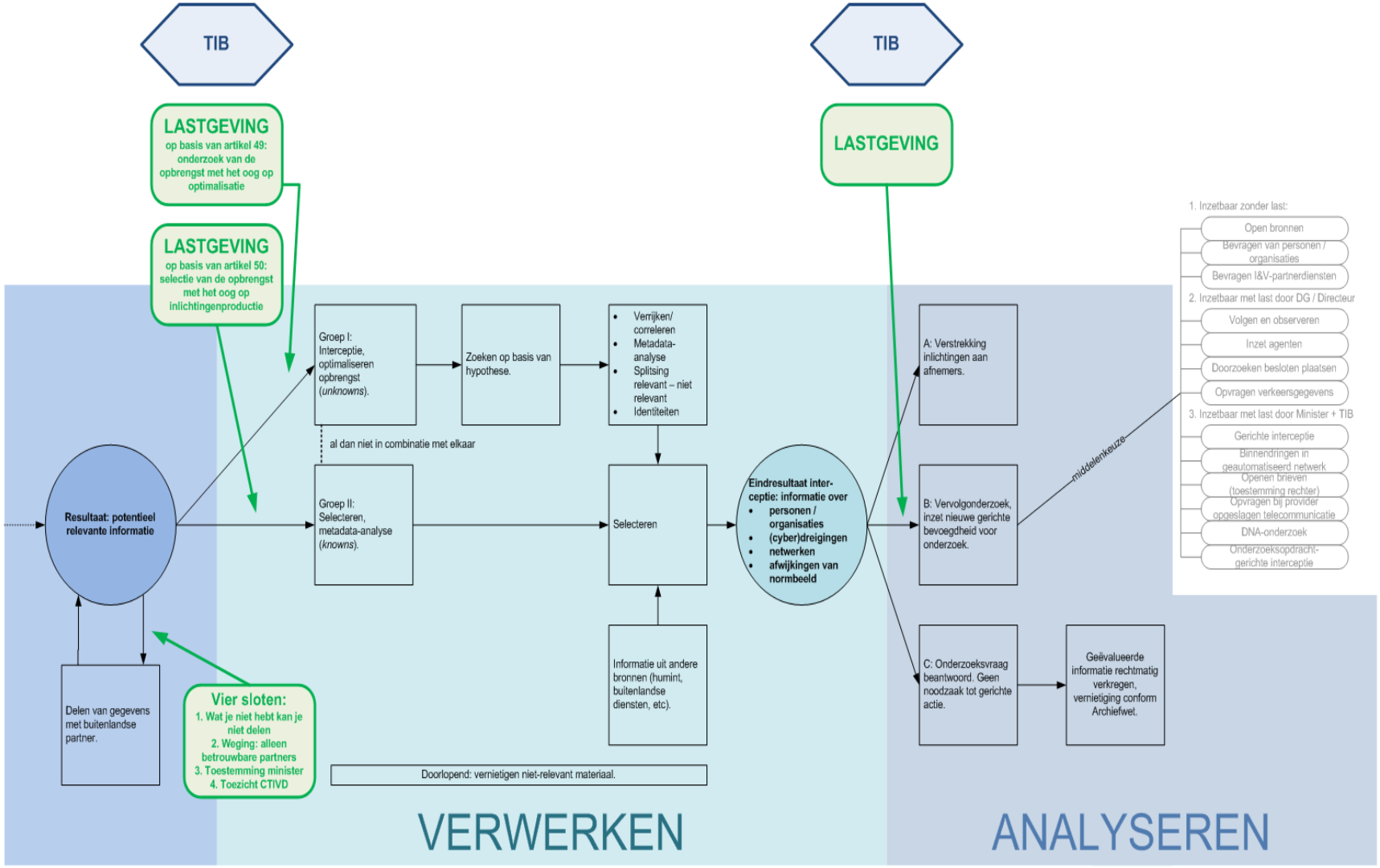
Opvragen verkeersgegevens bij aanbieder van communicatiediensten (artikel 55)	Minister of namens deze het hoofd van de dienst.	Max. 3 maanden; verlenging voor eenzelfde periode mogelijk.	Doel; noodzakelijkheid; proportionaliteit; subsidiariteit.	Een jaar, met eenmalige verlengingsmogelijkheid van zes maanden (artikel 27, eerste en derde lid).	Niet van toepassing.
Opvragen abonneegegevens bij aanbieder van communicatiediensten (artikel 56)	Geen toestemming vereist.	Niet van toepassing.	Doel; noodzakelijkheid; proportionaliteit; subsidiariteit.	Een jaar, met eenmalige verlengingsmogelijkheid van zes maanden (artikel 27, eerste en derde lid)	Niet van toepassing.
Medewerkingsplicht bij ontsleuteling gegevens verkregen op grond van artikel 47, eerste lid, en 48, eerste lid (artikel 57)[319]	Minister en toets TIB.	Max. 3 maanden; verlenging voor eenzelfde periode mogelijk.	Doel; noodzakelijkheid; proportionaliteit; subsidiariteit.	Niet van toepassing.	Niet van toepassing.
Toegang tot plaatsen (artikel 58)[320]	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 43, eerste lid, is alleen toegestaan door personen die daartoe door hoofd van de dienst zijn aangewezen.

[319] Ondersteunende bevoegdheid.
[320] Ondersteunende bevoegdheid.

Bijlage 4 Schematische weergave onderzoeksopdrachtgerichte interceptie



* Zie aparte matrix met een overzicht van alle (bijzondere) bevoegdheden en vereiste toestemmingsniveaus


TIB
TIB
LASTGEVING
op basis van artikel 49: onderzoek van de opbrengst met het oog op optimalisatie
LASTGEVING
op basis van artikel 50: selectie van de opbrengst met het oog op inlichtingenproductie
LASTGEVING
Groep I: Interceptie, optimaliseren opbrengst (unknowns).
Zoeken op basis van hypothese.
Verrijken/ correleren
Metadata-analyse
Splitsing relevant – niet relevant
Identiteiten
al dan niet in combinatie met elkaar
Resultaat: potentieel relevante informatie
Groep II: Selecteren, metadata-analyse (knowns).
Selecteren
Eindresultaat inter-ceptie: informatie over
personen / organisaties
(cyber)dreigingen
netwerken
afwijkingen van normbeeld
A: Verstrekking inlichtingen aan afnemers.
B: Vervolgonderzoek, inzet nieuwe gerichte bevoegdheid voor onderzoek.
middelenkeuze
1. Inzetbaar zonder last:
Open bronnen
Bevragen van personen / organisaties
Bevragen I&V-partnerdiensten
2. Inzetbaar met last door DG / Directeur
Volgen en observeren
Inzet agenten
Doorzoeken besloten plaatsen
Opvragen verkeersgegevens
3. Inzetbaar met last door Minister + TIB
Gerichte interceptie
Binnendringen in geautomatiseerd netwerk
Openen brieven (toestemming rechter)
Opvragen bij provider opgeslagen telecommunicatie
DNA-onderzoek
Onderzoeksopdracht-gerichte interceptie
C: Onderzoeksvraag beantwoord. Geen noodzaak tot gerichte actie.
Geëvalueerde informatie rechtmatig verkregen, vernietiging conform Archiefwet.
Informatie uit andere bronnen (humint, buitenlandse diensten, etc).
Delen van gegevens met buitenlandse partner.
Vier sloten:
1. Wat je niet hebt kan je niet delen
2. Weging: alleen betrouwbare partners
3. Toestemming minister
4. Toezicht CTIVD
Doorlopend: vernietigen niet-relevant materiaal.
VERWERKEN
ANALYSEREN
Toezicht door CTIVD

Bijlage 5 Schematisch overzicht wetgeving van enkele andere landen

Onderwerp	Duitsland	Verenigd Koninkrijk[1]	Frankrijk	België	Nederland (wetsvoorstel)
Toestemming interceptie					
• Wie verleent toestemming?	Minister	Minister	Premier	Minister	Minister
• Wie toetst?	G10-commissie	Commissioner	CNCTR	BIM-commissie	TIB
• Adviserend / bindend (A/B)	B	B	A	B	B
• Onderscheid binnen- en buitenland? wel (X) of geen (0)	X (buitenland geen G10-commissie)	X (buitenland geen Commissioner)	X (buitenland geen CNCTR)	X (buitenland geen BIM-commissie)	0
Toezicht					
• Wie houdt toezicht?	G10-commissie / PKGr	Commissioner / ISC	CNCTR	VCI	CTIVD / CIVD
• Adviserend of bindend (A/B)	B / A	A	A	B	A
• Onderscheid binnen- en buitenland? wel (X) of geen (0)	X (buitenland geen G10-commissie)	X (buitenland geen Commissioner)	X (buitenland geen CNCTR)	0	0
Klachtbehandeling					
• Wie behandelt klachten	Bestuursrechter	IPT	Conseil d'État	VCI	CTIVD
• Adviserend / bindend (A/B)	B	B	B	B	B
Bulkinterceptie					
• Toestemming buitenland	Ja	Ja	Ja	Ja	Ja
• Toestemming binnenland	Ja	Ja, enkel metadata	Ja	Nee	Ja
• Onderscheid kabel/niet-kabel?	Nee	Nee	Nee	Nee	Nee
• Bewaartermijn buitenland	Geen	Geen	4 jaar inhoud 6 jaar metadata	Geen	3 jaar
• Bewaartermijn binnenland	Restrictief regime[2]	Geen	Gedifferentieerd[3]	Nvt	3 jaar
• Onkostenvergoeding	Naar redelijkheid/ tarieven	Naar redelijkheid	Naar redelijkheid	Onbekend	Naar redelijkheid

[1] Met betrekking tot het VK is uitgegaan van het beschreven wetvoorstel.
[2] Verwerking van binnenlandse data geschiedt in beginsel op basis van voorafgaande toestemming (G-10) dat sterk lijkt op gerichte interceptie.
[3] Het varieert van 1 maand tot enkele jaren (cybersecurity) afhankelijk van de bevoegdheid op basis waarvan de gegevens zijn verkregen alsmede of het metadata dan wel ook inhoud betreft.