Reactie CTIVD

op het concept-wetsvoorstel Wet op de inlichtingen- en veiligheidsdiensten 20XX

(consultatieversie juni 2015)

26 augustus 2015

Commissie van Toezicht
op de Inlichtingen- en
Veiligheidsdiensten

Commissie van Toezicht
op de Inlichtingen- en
Veiligheidsdiensten

REACTIE

Concept-wetsvoorstel Wiv 20XX

Inhoudsopgave

Zie aparte bijlage bij deze reactie: rapport van Universiteit Leiden Het mensenrechtelijk kader voor het Nederlandse stelsel van toezicht op de inlichtingen- en veiligheidsdiensten (augustus 2015)

Commissie van Toezicht
op de Inlichtingen- en
Veiligheidsdiensten

VOGELVLUCHT

De reactie van de CTIVD in vogelvlucht

Op 1 juli 2015 ontving de Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (CTIVD) van de minister van Binnenlandse Zaken en Koninkrijksrelaties, mede namens de minister van Defensie, het concept-wetsvoorstel voor een nieuwe Wet op de inlichtingen- en veiligheidsdiensten (Wiv). Zij werd door de ministers in de gelegenheid gesteld haar reactie te geven op het voorstel.

De CTIVD ziet het als haar kernopdracht door middel van onafhankelijk toezicht op de rechtmatigheid van het handelen van de AIVD en de MIVD bij te dragen aan een goede balans tussen het belang van de nationale veiligheid en dat van de bescherming van de persoonlijke levenssfeer. De afgelopen jaren heeft de CTIVD in haar toezichtsrapporten verschillende knelpunten gesignaleerd waarbij naar haar oordeel die juiste balans niet altijd werd gevonden. Zij heeft hierover aanbevelingen gedaan aan de ministers. De CTIVD constateert met waardering dat een groot deel van die punten een plaats heeft gekregen in het concept-wetsvoorstel en/of de memorie van toelichting.

De CTIVD zal zich niet uitlaten over de (on)wenselijkheid van de voorgestelde uitbreiding van de bevoegdheden van de diensten. Dit valt buiten haar taak. Zij beperkt haar reactie tot de vraag of de privacy-waarborgen hierbij in voldoende mate zijn versterkt.

De gekozen benadering

Het concept-wetsvoorstel dat voorligt kent op een aantal punten een verruiming van de bevoegdheden van de diensten. Het gaat hierbij niet alleen om de uitbreiding van de interceptiebevoegdheden tot de kabel, maar ook om bijvoorbeeld de uitbreiding van de hackbevoegdheid en de bevoegdheid om data-analyse uit te voeren. Bij deze verruiming van de bevoegdheden van de AIVD en de MIVD hoort, zoals ook in het evaluatierapport van de commissie Dessens verwoord, een versterking van het onafhankelijk toezicht op de toepassing van deze bevoegdheden. Dat wil zeggen dat het toezicht zodanig moet zijn ingericht dat dit een effectieve, wezenlijke, waarborg vormt tegen de mogelijkheid van ongerechtvaardigde inbreuken op de privacy. Het uitgangspunt hierbij is dat hoe meer inbreuk de diensten mogen maken in termen van hoeveelheid en gevoeligheid van gegevens die worden verzameld en verwerkt, hoe belangrijker die waarborg wordt.

Het centrale onderwerp van de reactie van de CTIVD op het concept-wetsvoorstel is dan ook **effectief toezicht als waarborg tegen ongerechtvaardigde inbreuken op de privacy.**

Voor effectief toezicht zijn twee onderwerpen van belang: (1) de positie van de toezichthouder; deze moet onafhankelijk en onpartijdig zijn, met toegang tot alle informatie bij de diensten en met de mogelijkheid dwingend in te grijpen bij overtreding van de regels en (2) een wettelijk normenkader dat duidelijke en concrete aanknopingspunten biedt om het handelen van de diensten ook daadwerkelijk op rechtmatigheid te kunnen toetsen. Deze vereisten volgen uit het Europees en internationaal mensenrechtelijk kader voor toezicht op de inlichtingen- en veiligheidsdiensten. Dit vertaalt zich bij de beoordeling van het concept-wetsvoorstel naar de volgende twee vragen: **(1) Wordt de positie van de CTIVD als toezichthouder voldoende versterkt?** En **(2) Biedt het voorgestelde normenkader voldoende houvast voor toezicht?** Deze vragen komen aan de orde in de hoofdstukken 1 en 2 van de reactie van de CTIVD en worden hieronder in het kort beantwoord.

Bij het bestuderen van het concept-wetsvoorstel en de memorie van toelichting is de CTIVD ook tegen onderwerpen aangelopen die niet zozeer vanuit het oogpunt van effectief toezicht, maar meer in het algemeen voor de bescherming van de privacy van belang zijn. De vraag die de CTIVD zich daarbij heeft gesteld is: **(3) Waar ontbreken nog adequate waarborgen voor de bescherming van de privacy?** Deze vraag vormt het onderwerp van hoofdstuk 3 van haar reactie.

In hoofdstuk 4 van haar reactie plaatst de CTIVD een aantal wetstechnische ofwel tekstuele opmerkingen.

Wordt de positie van de CTIVD als toezichthouder voldoende versterkt?

Het antwoord op deze vraag is kort gezegd: nee, de voorgestelde bevoegdheden van de CTIVD schieten tekort. Uit de geldende Europees en internationaal mensenrechtelijke normen blijkt dat een verdergaande versterking van de positie van de CTIVD nodig is dan nu wordt voorgesteld, wil er sprake zijn van effectief toezicht. Het voornaamste gebrek is dat de CTIVD geen bindend rechtmatigheidsoordeel toekomt bij de toepassing van de meest inbreukmakende bijzondere bevoegdheden door de diensten, zoals de afluisterbevoegdheid en de hackbevoegdheid. Men zou kunnen stellen dat de toezichthouder in het voorstel voldoende tanden mist.

De CTIVD baseert dit standpunt onder meer op een studie die recent door de universiteit Leiden is verricht, waartoe zij opdracht heeft gegeven (zie de aparte **bijlage** bij deze reactie).

In het concept-wetsvoorstel ligt het zwaartepunt van de wijzigingen op het gebied van het toezicht bij de klachtbehandeling. Voorgesteld wordt de CTIVD te positioneren als een externe klachtbehandelaar, in plaats van een interne klachtenadviescommissie die de minister adviseert. De uiteindelijke, bindende beslissing op klachten over activiteiten van de diensten komt daarmee bij de CTIVD te liggen en dus niet meer zoals nu het geval is bij de minister. Dit is zonder meer een goede ontwikkeling. Waar het gaat om het rechtmatigheidstoezicht op de werkzaamheden van de diensten (en dat is, buiten de klachtbehandeling, 90% van het werk) wijzigt de positie van de CTIVD slechts in beperkte mate. Voor de inbreukmakende bijzondere bevoegdheden van de diensten (denk aan telefoontaps of het hacken van een pc) komt er een heroverwegingsplicht, die inhoudt dat de minister zijn toestemming voor uitoefening van die bevoegdheid opnieuw moet bezien als de CTIVD tot een onrechtmatigheidsoordeel komt. Als de minister dan bij zijn eerdere besluit blijft, is hij verplicht de commissie voor de Inlichtingen- en Veiligheidsdiensten van de Tweede Kamer (CIVD) en de CTIVD daarvan op de hoogte te brengen. Het oordeel van de CTIVD bindt de minister dus niet. De heroverwegingsplicht introduceert slechts een hogere drempel voor de ministers.

In de visie van de CTIVD gaat dit voorstel voorbij aan de werkelijke functie van het rechtmatigheids-toezicht op de inzet van heimelijke bevoegdheden die inbreuk maken op de privacy. In het Nederlandse systeem is de CTIVD de enige externe partij die volledige inzage heeft in wat de diensten doen. Zij heeft daardoor de mogelijkheid de activiteiten van de AIVD en de MIVD ook daadwerkelijk te toetsen aan de kaders die door de wetgever zijn opgelegd. Het toezicht dat zij uitoefent vervangt in feite de mogelijkheid van een door de burger in te roepen rechtsmiddel tegen de inbreuk op zijn privacy, nu die burger vanwege het heimelijke karakter daarvan doorgaans geen kennis heeft of zal krijgen van die inbreuk. Dit brengt mee dit toezicht als geheel en niet alleen op het punt van klachtbehandeling moet kunnen dienen als een *"effective remedy"* in de zin van artikel 13 in combinatie met artikel 8 van het EVRM. Als de CTIVD de inzet van een heimelijke bevoegdheid onrechtmatig acht, moet dit naar haar oordeel dan ook meer zijn dan een hogere drempel waar de minister overheen moet stappen; de deur moet dan dicht. De CTIVD moet daarbij ook kunnen opleggen dat een operatie wordt beëindigd en dat de onrechtmatig verzamelde gegevens worden vernietigd.

Bindend *ex post* rechtmatigheidstoezicht tast de ministeriële verantwoordelijkheid en de parlementaire controle op het (beleidsmatig) handelen van de diensten niet aan. Het toezicht van de CTIVD richt zich op een juridische beoordeling van de autorisatie en van de uitvoering van bijzondere bevoegdheden en niet op de doelmatigheid of doeltreffendheid van het gevoerde beleid en de uitvoering ervan. Ook op andere terreinen kan een minister in de uitvoering van zijn beleid begrensd worden door oordelen van externe onafhankelijke instanties, terwijl hij in de richting van het parlement geheel verantwoordelijk blijft voor de uitvoering van zijn beleid.

Biedt het normenkader voldoende houvast voor toezicht?

De CTIVD constateert dat het wettelijk kader dat wordt voorgesteld voor de inzet van bijzondere bevoegdheden, op onderdelen onvoldoende duidelijkheid biedt voor effectief toezicht. De meeste vragen rijzen ten aanzien van het stelsel voor grootschalige interceptie (bulk). De CTIVD heeft op basis van de beschrijving in de memorie van toelichting van het voorgestelde 'driefasenmodel', een fictieve casus geschreven om zicht te krijgen op hoe het stelsel in de praktijk zou kunnen werken. De CTIVD constateert hierbij dat het concept-wetsvoorstel op verschillende punten onvoldoende duidelijkheid biedt over de reikwijdte en de onderlinge samenhang van de bevoegdheden. Zo zijn de verschillende vormen van technisch en inhoudelijk onderzoek van de diensten niet duidelijk afgebakend. Het is voor de CTIVD ook de vraag hoe de diensten intern vorm zullen geven aan de motivering van de selectie van communicatie uit de geïntercepteerde bulk op het niveau van personen en/of organisaties. Hiervoor is in het voorgestelde stelsel in ieder geval geen toestemming van de minister meer vereist, waar dat nu wel het geval is.

Waar ontbreken adequate waarborgen voor de bescherming van de privacy?

Een onderwerp dat centraal staat in dit onderdeel van de reactie (hoofdstuk 3) is de bewaartermijn voor de verschillende soorten verzamelde gegevens. Na verloop van deze termijn dienen gegevens te worden vernietigd. Het Hof van Justitie van de EU heeft in 2014 bepaald dat een bewaartermijn voor opgeslagen (persoons)gegevens niet langer mag zijn dan strikt noodzakelijk is en dat dit aan de hand van objectieve criteria moet worden vastgesteld. De CTIVD stelt vast dat de voorgestelde bewaartermijnen – één jaar voor gericht verzamelde gegevens en drie jaar voor bulk – lang tot zeer lang zijn. De in de memorie van toelichting gegeven motivering voor de lengte van de voorgestelde bewaartermijnen overtuigt niet, gegeven de voorwaarden die het Hof van Justitie van de EU daaraan stelt.

Een ander belangrijk punt betreft de uitbreiding van de hackbevoegdheid. De CTIVD vindt dat de mogelijkheid die het concept-wetsvoorstel de diensten biedt voor het binnendringen van een geautomatiseerd werk van een derde, om informatie over een target te vergaren, niet met voldoende waarborgen is omkleed.

Naast de hierboven besproken onderwerpen, plaatst de CTIVD in haar onderstaande reactie kanttekeningen bij de bepalingen die zien op de samenwerking met buitenlandse inlichtingen- en veiligheidsdiensten, op geautomatiseerde data-analyse, op de uitbreiding van de bevoegdheid tot het bevorderen of treffen van maatregelen en op de bepaling over het vernietigen van de gegevens betreffende informanten en agenten.

REACTIE

Concept-wetsvoorstel Wiv 20XX

1. Toezicht en klachtbehandeling

1.1 Inleiding

De CTIVD acht versterking van het bestaande toezicht op de inlichtingen- en veiligheidsdiensten van essentieel belang. Hierbij speelt een aantal overwegingen een rol.

- Het publiek vertrouwen in het optreden van de inlichtingen- en veiligheidsdiensten staat onder druk. Onthullingen over het functioneren van met name buitenlandse diensten die de grenzen van hun wettelijke bevoegdheden zouden hebben overschreden, zijn hier een belangrijke aanjager voor geweest.
- Europees en internationaal mensenrechtelijke normen stellen in toenemende mate (directe of indirecte) eisen aan het toezicht op inlichtingen- en veiligheidsdiensten.
- Daar komt bij de discussie over een uitbreiding van de interceptiebevoegdheden van de AIVD en de MIVD. Onder invloed van maatschappelijke en technologische ontwikkelingen verandert het karakter van bedreigingen van de nationale veiligheid (mondiale impact van terrorisme, verschuivende machtsverhoudingen, meer militaire uitzendingen, nieuwe bedreigingen via cyber) en doet zich een verschuiving voor naar moderne communicatiekanalen (kabel i.p.v. satelliet en HF-radio, meer mondiale connectie door internet en sociale media). Om de nationale veiligheid afdoende te kunnen blijven beschermen achten de regering en de diensten het noodzakelijk ook in cyber en het kabelgebonden domein voldoende interceptiebevoegdheden te hebben.

De voorgaande omstandigheden geven aanleiding tot een te versterken inrichting van het toezicht op de AIVD en de MIVD. In haar reactie van 10 maart 2014 aan de Tweede Kamer op het evaluatierapport van de Commissie Dessens heeft de CTIVD dit belang al onderstreept. Hierbij heeft de CTIVD benadrukt dat versterking van het toezicht reeds een opzichzelfstaande noodzaak is, ongeacht de uitbreiding van de interceptiebevoegdheden van de diensten.

In dit hoofdstuk staat de vraag centraal: **Wordt de positie van de CTIVD als toezichthouder op de inlichtingen- en veiligheidsdiensten in het concept-wetsvoorstel voldoende versterkt?**

De memorie van toelichting bij het concept-wetsvoorstel Wiv 20XX wijst op de noodzaak van versterking van het bestaande toezicht. Deze wordt gevonden in een samenstel van maatregelen waarmee naar het oordeel van de regering aan de eisen van het Europees Verdrag ter bescherming van de Rechten van de Mens en de Fundamentele Vrijheden (hierna: EVRM) wordt voldaan.

- Voor wat betreft de toezichthoudende taak van de CTIVD wordt een heroverwegingsplicht voor de ministers voorgesteld. (artikel 102 lid 3 concept-wetsvoorstel).

- Daarnaast wordt de CTIVD in het concept-wetsvoorstel als een zelfstandige, onafhankelijke, klachtinstantie gepositioneerd die bindende oordelen in klachtzaken kan geven (artikel 103 e.v. concept-wetsvoorstel). De CTIVD komt in de plaats van de Nationale ombudsman als externe klachtinstantie. De betrokken minister blijft verantwoordelijk voor de interne klachtprocedure, waarin de CTIVD dan geen rol meer heeft als klachtenadviescommissie.
- Tot slot wordt een klokkenluidersregeling geïntroduceerd en bij de CTIVD ondergebracht (artikel 114 e.v. concept-wetsvoorstel).
- Vanwege de voorgestelde klachtenregeling en klokkenluidersregeling, is in het concept-wetsvoorstel een institutionele scheiding (functioneel, personeel en organisatorisch) binnen de CTIVD tussen de toezichthoudende taak en de twee andere taken opgenomen. Deze voorziening wordt noodzakelijk geacht om een onbevooroordeelde oordeelsvorming te waarborgen.

Naar het oordeel van de CTIVD vindt echter met het bovenstaande onvoldoende versterking van het toezicht plaats. De regering gaat in het concept-wetsvoorstel voorbij aan een aantal belangrijke Europees- en internationaal mensenrechtelijke ontwikkelingen en eisen voor effectief toezicht op inlichtingen- en veiligheidsdiensten, zoals die onder meer uit de jurisprudentie van het EHRM volgen. Niet alleen wordt hierdoor onvoldoende recht gedaan aan het belang het publiek vertrouwen in het werk van de AIVD en de MIVD te waarborgen, ook bestaat hierdoor gerede twijfel over de juridische houdbaarheid van het concept-wetsvoorstel op dit punt op de middellange termijn. De CTIVD hecht eraan bij deze gelegenheid de door haar geconstateerde knelpunten nader toe te lichten.

Het toezicht en de controle op de inlichtingen- en veiligheidsdiensten kent zowel een interne[1] als een externe dimensie[2]. De CTIVD richt zich hier alleen op de elementen in het concept-wetsvoorstel over het externe toezicht die haar eigen taken, positie en organisatie betreffen (rechtmatigheidstoezicht en klachtbehandeling).

In dit hoofdstuk komen de volgende onderwerpen in genoemde volgorde aan de orde:
- Toezicht op rechtmatigheid
  - Versterking ex post toezicht CTIVD (heroverwegingsplicht)
  - *Ex ante* toetsing (ministeriële toestemming)
- Institutionele scheiding CTIVD
- Enkele bevoegdheden CTIVD
  - Beoordeling staatsgeheime karakter van informatie
  - Geheimhoudingsplicht oud-medewerkers
- Gevolgen voor de organisatie en werkwijze van de CTIVD

De adviezen van de CTIVD zijn in de tekst telkens in een **kader** weergegeven.

[1] Intern toezicht/controle: De verantwoordelijke ministers (van BZK en Defensie), de coördinator van de inlichtingen- en veiligheidsdiensten (SG van AZ), Comité Verenigde Inlichtingendiensten Nederland (CVIN, in het concept-wetsvoorstel gewijzigd in Commissie Veiligheids- en Inlichtingendiensten Nederland).

[2] Extern toezicht/controle: CTIVD, Parlement, Nationale ombudsman, rechter.

1.2 Toezicht op rechtmatigheid

[Artikel 102; p. 162-163 MvT]

Inleiding

Het toezicht van de CTIVD op de inlichtingen- en veiligheidsdiensten maakt onderdeel uit van een breder stelsel van toezicht en controle door externe instanties. Dit stelsel blijft in het concept-wetsvoorstel grotendeels ongewijzigd. Alleen het rechtmatigheidstoezicht van de CTIVD en de behandeling van klachten (nu door de CTIVD als klachtenadviescommissie en de Nationale ombudsman als externe instantie) wordt herzien. De wijze waarop dit volgens het concept-wetsvoorstel dient te gebeuren, is echter ontoereikend, met name in het licht van Europees en internationaal mensenrechtelijke normen voor effectief toezicht op inlichtingen- en veiligheidsdiensten, zoals die onder meer uit de jurisprudentie van het EHRM volgen.

Bij de bespreking van het toezicht op de rechtmatigheid komen twee onderwerpen aan de orde. Eerst wordt ingegaan op de wijze waarop in het voorstel invulling wordt gegeven aan de versterking van het *ex post* (achteraf) rechtmatigheidstoezicht van de CTIVD. Daarna op de wijze waarop in het voorstel invulling wordt gegeven aan de *ex ante* (vooraf) toetsing van de inzet van bijzondere bevoegdheden. Aan klachtbehandeling wordt verderop in deze reactie afzonderlijk aandacht besteed.

1.2.1 Versterking ex post toezicht: heroverwegingsplicht

Concept-wetsvoorstel

In het concept-wetsvoorstel wordt de versterking van het toezicht van de CTIVD op de toestemmingsverlening van de minister gezocht in de invoering van een heroverwegingsplicht voor de minister. Dit geldt voor de bijzondere bevoegdheden waarvoor de minister volgens het concept-wetsvoorstel persoonlijk toestemming dient te geven. Als de CTIVD – desgewenst direct na de toestemmingsverlening – aan de minister mededeelt dat de toestemming naar haar oordeel onrechtmatig is, dan dient de minister de toestemming opnieuw te bezien. Mocht de minister van oordeel zijn dat de toestemming gehandhaafd moet blijven, dan dient hij onverwijld de CTIVD en de CIVD hiervan op de hoogte te stellen. Volgens de memorie van memorie van toelichting kan de CIVD de minister dan desgewenst ter verantwoording roepen. Met deze inrichting is volgens de regering sprake van een sluitend stelsel. De memorie van toelichting licht toe dat in dit stelsel de ministeriële verantwoordelijkheid intact blijft en tegelijkertijd wordt voorkomen dat er praktijken ontstaan die onrechtmatig zijn zonder dat dit is getoetst. Volgens de regering is met deze regeling bovendien voldaan aan de vereisten van het Europees Hof voor de Rechten van de Mens (hierna: EHRM), nu de toezichthouder (CTIVD) in staat is daadwerkelijk effectief toezicht te houden. De verdere versterking van de al vergaande bevoegdheden van de CTIVD met de invoering van een meldingsmogelijkheid en de daarmee corresponderende heroverwegingsplicht voor de minister dragen hier volgens de regering in voldoende mate aan bij.

Evaluatiecommissie Dessens

Het concept-wetsvoorstel neemt de aanbeveling van de evaluatiecommissie Dessens voor bindende rechtmatigheidsoordelen over de ministeriële toestemming voor bepaalde bijzondere bevoegdheden niet over.

Naar aanleiding van de aanbeveling van de commissie Dessens[3] is de focus van de herziening van het rechtmatigheidstoezicht van de CTIVD komen te liggen bij het toezicht op de toestemmingsverlening voor de inzet van bijzondere bevoegdheden. De reden hiervoor is dat de commissie Dessens de uitbreiding van de (ongerichte) interceptiebevoegdheden van de AIVD en de MIVD koppelt aan een versterking van het toezicht op de toepassing ervan. Deze versterking heeft zij gezocht in de bevoegdheid van de CTIVD om, direct na een verleende ministeriële toestemming voor de inzet van interceptiebevoegdheden, bindende oordelen over de rechtmatigheid van de toestemming te kunnen geven. De commissie Dessens heeft de bindende rechtmatigheidsoordelen niet alleen aanbevolen voor de interceptiebevoegdheden, maar voor alle bijzondere bevoegdheden waarvoor ministeriële toestemming vereist is of zou moeten zijn.[4]

Europees en internationaal (mensen)rechtelijk kader

De CTIVD heeft een aantal vooraanstaande wetenschappers op het gebied van staats- en bestuursrecht en mensenrechten, verzocht een studie te verrichten naar het Europees en internationaal mensenrechtelijke kader voor de inrichting van het toezicht op de inlichtingen- en veiligheidsdiensten, en in het bijzonder naar de vraag of het voldoende is alleen het klachtoordeel van de CTIVD bindende kracht te geven en niet (ook) de rechtmatigheidsoordelen.[5] U vindt het rapport als bijlage bij deze reactie. De uitkomst van dit onderzoek vormt de grondslag voor het standpunt van de CTIVD dat effectief toezicht vereist dat, naast bindende klachtoordelen, ook de rechtmatigheidsoordelen over de inzet van (bepaalde) bijzondere bevoegdheden bindend dienen te zijn.

In de EHRM-jurisprudentie wordt de noodzaak onderstreept van onafhankelijk *ex post* (achteraf) toezicht om te controleren of de uitvoering van een (heimelijke) onderzoeksbevoegdheid van de inlichtingen- en veiligheidsdiensten geschiedt op een manier die binnen de wettelijke, mensenrechtelijke en in de toestemmingsverlening aangegeven grenzen blijft. Deze noodzaak hangt sterk samen met de aard van het werk van de inlichtingen- en veiligheidsdiensten. Dit vindt immers doorgaans in het geheim plaats. Voor de burgers of organisaties tegen wie onderzoeksbevoegdheden worden ingezet is het daarmee grotendeels onmogelijk zelf enigerlei vorm van rechtmatigheidscontrole in gang te zetten. Het belang van ex post toezicht is erin gelegen dat gedurende de gehele looptijd van een geautoriseerde inzet van een bepaalde bijzondere bevoegdheid moet kunnen worden gekeken of dit binnen de juridische grenzen wordt uitgevoerd.[6]

Hoewel de jurisprudentie van het EHRM niet expliciet aangeeft dat het *ex post* toezicht dient te resulteren in bindende oordelen, wijzen recente uitspraken onmiskenbaar wel in die richting.[7] Hiervoor benoemt het rapport een aantal argumenten:

---

3 *Naar een nieuwe balans tussen bevoegdheden en waarborgen*, evaluatie Wet op de inlichtingen- en veiligheidsdiensten, commissie Dessens, december 2013, *Kamerstukken II* 2013-2014, 33 820, nr. 1.

4 In ieder geval voor gebruik van (gericht/ongericht) geïntercepteerde kabel en niet-kabelgebonden communicatie (vervanging van huidige artikelen 25-27 Wiv 2002), toepassing van registratie- en observatiemiddelen in woning (huidige artikel 20 lid 3), doorzoeken van woningen (huidige artikel 22 lid 6) en hacken (huidige artikel 24); *Naar een nieuwe balans tussen bevoegdheden en waarborgen*, evaluatie Wet op de inlichtingen- en veiligheidsdiensten, commissie Dessens, december 2013, *Kamerstukken II* 2013-2014, 33 820, nr. 1, p. 82-84.

5 *Het mensenrechtenkader voor het Nederlandse stelsel van toezicht op de inlichtingen- en veiligheidsdiensten*, J.P. Loof, J. Uzman, T. Barkhuysen, A.C. Buyse, J.H. Gerards & R.A. Lawson, augustus 2015, te raadplegen via www.ctivd.nl.

6 *Ibidem*, p. 15-16.

7 *Ibidem*, p. 16.

- De eis van bindende rechtmatigheidsoordelen valt te destilleren uit de voorwaarden die in de EHRM-jurisprudentie voortvloeien uit artikel 8 (privéleven) in samenhang met artikel 13 EVRM (effectief rechtsmiddel). Ter invulling van de effectiviteitsvereisten uit artikel 13 EVRM vereist het EHRM dat een onafhankelijke instantie bindende oordelen kan geven in klachtprocedures over inlichtingen- en veiligheidsdiensten.[8] Een effectief rechtsmiddel vereist in dit verband dat de onafhankelijke instantie voldoende onderzoeksbevoegdheden en –mogelijkheden heeft om alle gegevens in te zien ter beoordeling van de rechtmatigheid van de heimelijke informatieverzameling of communicatieonderschepping en daarover een eigen juridisch bindend oordeel uit te spreken, dat waar nodig dwingt tot aanpassing of vernietiging van de verzamelde gegevens.[9] Het ligt voor de hand deze eis met betrekking tot de behandeling van klachten door te trekken naar het rechtmatigheidstoezicht. Anders zou dat grote afbreuk doen aan de effectiviteit van dat toezicht. Ex post toezicht dient vooral ook als plaatsvervanger van een door de betrokkene in te roepen rechtsmiddel (klacht), nu deze dat zelf niet kan omdat hij onwetend is over de jegens hem gepleegde privacy-inbreuk. Vanuit dit oogpunt is het logisch de effectiviteitseisen zoals die geformuleerd zijn voor klachtprocedures naar analogie toe te passen op ex post rechtmatigheidstoezicht dat plaatsvindt los van enige ingediende klacht.[10]
- Naast *ex post* toezicht heeft het EHRM zich ook uitgelaten over de fase van toestemmingsverlening voor de inzet van heimelijke onderzoeksbevoegdheden die diep ingrijpen in de persoonlijke levenssfeer van burgers. Het EHRM heeft een voorkeur voor *ex ante* (vooraf) toestemmingsverlening door een onafhankelijke autoriteit. Dit kan de rechter zijn, maar dat hoeft niet.[11] Van belang is dat het gaat om een onafhankelijke externe instantie, die qua onafhankelijkheid en uitspraakbevoegdheden (bindende oordelen) vergelijkbaar is met een rechter en die algehele toegang heeft tot alle relevante staatsgeheime informatie. Het EHRM is nog nooit zover gegaan *ex ante* toestemmingsverlening als een expliciete eis voor EVRM-conformiteit te formuleren. Uit de jurisprudentie kan wel de volgende harde lijn worden gedestilleerd: Als de inzet van een heimelijke onderzoeksbevoegdheid *ex ante* (vooraf) is getoetst op rechtmatigheid en mensenrechtenconformiteit door een onafhankelijke instantie, dan dient het *ex post* (achteraf) toezicht te zien op de uitoefening van de bevoegdheid en de vraag of binnen de grenzen van de toestemming is gebleven (zie ook de vorige bullet).[12] Echter, indien er geen sprake is van een *ex ante* (vooraf) toets door een onafhankelijke instantie, zoals in het concept-wetsvoorstel aan de orde is, dan ligt het voor de hand dat het *ex post* (achteraf) toezicht mede een bindend oordeel moeten kunnen omvatten over de gegeven autorisatie door de minister.[13]

---

8 *Ibidem*, p. 6-7.

9 *Ibidem*, p. 7.

10 *Ibidem*, p. 16.

11 *Ibidem*, p. 13.

12 *Ibidem*, p. 15.

13 *Ibidem*, p. 18.

- In gezaghebbende analyses van onder meer de *Venice Commission* van de Raad van Europa (2007)[14] en de *Independent Reviewer of Terrorism Legislation* in het Verenigd Koninkrijk (2015)[15] wordt het principe van ministeriële verantwoordelijkheid en de daarmee samenhangende verantwoordingsplicht jegens het parlement in het algemeen niet als een voldoende waarborg voor de mensenrechtenconformiteit van het optreden van de inlichtingen- en veiligheidsdiensten gezien. Deze analyses bouwen voort op de jurisprudentie van het EHRM. Het EHRM wijdt hier zelf (nog) geen expliciete overwegingen aan. Volgens de genoemde rapporten is parlementaire controle van belang, maar zou in aanvulling hierop rechtmatigheidscontrole door een onafhankelijke gespecialiseerde toezichthouder dienen plaats te vinden. De toegevoegde waarde van bindend *ex post* toezicht door een gespecialiseerde onafhankelijke toezichthouder gedurende heimelijke informatieverzamelingsoperaties is vooral gelegen in het politiek neutrale, langdurige en continue karakter daarvan.[16] Bovendien is hiermee gewaarborgd dat een onafhankelijke instantie bij onrechtmatigheden dwingend kan ingrijpen en verzamelde gegevens kan laten vernietigen. Dit onderscheidt deze vorm van toezicht van het parlementaire toezicht op de inlichtingen- en veiligheidsdiensten.
- Het EHRM gaat er in zijn jurisprudentie vanuit dat bepaalde gebreken in het algemene systeem van rechtmatigheidstoezicht op de inlichtingen- en veiligheidsdiensten in de bijzondere omstandigheden van het geval door een andere vorm van rechtmatigheidscontrole kunnen worden gecompenseerd. Het EHRM weegt daarbij bijvoorbeeld ook mee welke mogelijkheden de rechter heeft om een oordeel over de rechtmatigheid van heimelijke interceptie of informatieverzameling uit te spreken, indien iemand op basis van de aldus verzamelde informatie strafrechtelijk vervolgd wordt of een beslissing die op basis van die informatie is genomen aanvecht in een bestuursrechtelijke of civiele procedure.[17] Voor de Nederlandse situatie dient er echter op te worden gewezen dat het vangnet van rechterlijke toetsing van het optreden van inlichtingen- en veiligheidsdiensten slechts een beperkte waarde heeft.[18] De reden is dat het de minister is die uiteindelijk gaat over de geheimhouding van informatie van de diensten (nu artikel 87 Wiv 2002; concept-wetsvoorstel artikelen 126 en 127).

Aandachtspunten

De CTIVD ziet met name een knelpunt in de wijze waarop in het concept-wetsvoorstel het rechtmatigheidstoezicht van de CTIVD op de toestemmingsverlening voor de inzet van de meest inbreukmakende bijzondere bevoegdheden wordt versterkt. Hierbij is niet, overeenkomstig de aanbeveling van de evaluatiecommissie Dessens, gekozen voor bindende rechtmatigheidsoordelen van de CTIVD, maar voor een systeem van heroverweging door de ministers, aangevuld met parlementaire controle. Anders dan de regering stelt, is deze regeling naar het oordeel van de CTIVD niet in overeenstemming met Europees en internationaal mensenrechtelijke normen over effectief toezicht op inlichtingen- en veiligheidsdiensten, zoals die onder meer uit de jurisprudentie van het EHRM volgen. Het beslisprimaat blijft bij de betrokken ministers.

---

[14] European Commission for Democracy through Law (Venice Commission), *Report on the Democratic Oversight of the Security Services*, adopted at its 71st Plenary Session, CDL-AD(2007)016, Strasbourg 11 June 2007.

[15] *A Question of Trust*, Report of the Investigatory Powers Review by David Anderson Q.C., Independent Reviewer of Terrorism Legislation, Presented to the Prime Minister pursuant to section 7 of the Data Retention and Investigatory Powers Act 2014, London June 2015.

[16] *Het mensenrechtenkader voor het Nederlandse stelsel van toezicht op de inlichtingen- en veiligheidsdiensten*, J.P. Loof, J. Uzman, T. Barkhuysen, A.C. Buyse, J.H. Gerards & R.A. Lawson, augustus 2015, p. 13, te raadplegen via www.ctivd.nl.

[17] *Ibidem*, p. 16, 19

[18] *Ibidem*, p. 19.

Effectief toezicht vereist echter de bevoegdheid van een onafhankelijke toezichthouder om bij onrechtmatig optreden in te grijpen. Daarmee worden niet alleen ongerechtvaardigde inbreuken op bepaalde mensenrechten voorkomen, ook vormt dit de basis voor het publiek vertrouwen in het werk van de AIVD en de MIVD. Parlementaire controle zoals die in het concept-wetsvoorstel bij de CIVD wordt neergelegd, vormt hiervoor geen afdoende vervangende maatregel. Dit is immers geen onafhankelijk juridisch oordeel. Het onvoldoende opvolgen van Europees en internationaalrechtelijke ontwikkelingen en vereisten maakt het concept-wetsvoorstel daarmee zeer kwetsbaar voor reeds de middellange termijn. De inrichting van een nieuwe wet is een tijdrovend proces dat vraagt om oplossingen en maatregelen die langere tijd houdbaar zijn. Het is ook onwenselijk gezien de belangen van nationale veiligheid en privacy die in de nieuwe wet in een juiste verhouding gewaarborgd moeten worden en het publieke vertrouwen dat daarmee gemoeid is.

Advies

Het rechtmatigheidstoezicht van de CTIVD wordt in het concept-wetsvoorstel in onvoldoende mate versterkt. Hiermee wordt niet voldaan aan de vereisten die onder meer het EHRM stelt aan effectief toezicht.

De CTIVD adviseert tot de invoering van een *ex post* bindend oordeel over de rechtmatigheid van de lastgeving voor de inzet van een bijzondere bevoegdheid en over de daaropvolgende uitvoering ervan (bv. verwerking gegevens; delen van data; bewaren). Hierbij merkt zij op dat zij een dergelijk oordeel in ieder geval voor de meest inbreukmakende bijzondere bevoegdheden noodzakelijk acht.

1.2.2 *Ex ante* toetsing: ministeriële toestemming

Inleiding

In aansluiting op het voorgaande acht de CTIVD het van belang nader in te gaan op de inrichting van de *ex ante* (vooraf) controle op de inzet van bijzondere bevoegdheden in het concept-wetsvoorstel. Hierbij gaat het met name om de verlening van toestemming voor de inzet van bijzondere bevoegdheden. Dit kan plaatsvinden door de verantwoordelijke minister of evenzeer in handen worden gelegd van een onafhankelijke externe partij. Dat wil zeggen een partij die geen politiek-bestuurlijke betrokkenheid en verantwoordelijkheid heeft voor de diensten. De toetsing vindt plaats voordat een bijzondere bevoegdheid daadwerkelijk wordt ingezet. Daarom wordt gesproken van preventieve of *ex ante* toetsing.

Concept-wetsvoorstel

Evenals nu het geval is, blijft toestemmingsverlening voor de inzet van bijzondere bevoegdheden primair in handen van de minister die voor de desbetreffende dienst verantwoordelijk is. Voor een aantal bijzondere bevoegdheden dient de toestemming persoonlijk door de minister te worden verleend.[19] In de overige gevallen is mandaat mogelijk. In het concept-wetsvoorstel is dus in de regel niet gekozen voor *ex ante* (voorafgaande) toestemmingsverlening door een onafhankelijke partij. Dit is overigens wel het geval, evenals nu, voor het openen van brieven en zendingen. Voordat deze bijzondere bevoegdheid mag worden toegepast, dient de rechter toestemming te geven. In het concept-wetsvoorstel is een vergelijkbare regeling getroffen voor de inzet van bijzondere bevoegdheden tegen een journalist, mits de inzet is gericht op het achterhalen van zijn bron.

[19] Bijzondere bevoegdheden waarvoor de minister toestemming moet verlenen (artikelen verwijzen naar het wetsontwerp): artikelen 25, tweede lid (toepassing observatie- en registratiemiddelen in woningen), 27, derde lid (doorzoeken van woningen), 28, tweede en vierde lid (DNA-onderzoek; verdere verwerking resultaten DNA-

Europees en internationaal (mensen)rechtelijke kader

Uit het rapport van de wetenschappelijke onderzoeksgroep van de universiteit Leiden blijkt dat het EHRM als hoofregel grote waarde hecht aan *ex ante* (vooraf) toestemmingsverlening voor bepaalde onderzoeksbevoegdheden, zoals interceptieoperaties, door een onafhankelijke, bij voorkeur rechterlijke, autoriteit. In aanvulling hierop acht het EHRM onafhankelijk *ex post* toezicht noodzakelijk om te controleren of de uitvoering van de interceptie geschiedt op een manier die binnen de wettelijke, mensenrechtelijke en in de toestemmingsverlening aangegeven grenzen blijft. Bij de inrichting van het *ex ante* toezicht, plaatst het rapport echter een aantal kanttekeningen:

- Het is van belang de voorkeur van het EHRM voor rechterlijke betrokkenheid niet te verabsoluteren. Niet alleen laat het EHRM ruimte voor een andere vorm van onafhankelijk toezicht, bijvoorbeeld door een gespecialiseerde toezichthouder. Het EHRM beoordeelt ook altijd het totaalpakket van aanwezige waarborgen en rechtsbeschermingsmechanismen rondom inlichtingen- en veiligheidsdiensten. Dat houdt in dat als er geen sprake is van een *ex ante* (vooraf) toets door een onafhankelijke instantie, zoals in het concept-wetsvoorstel aan de orde is, het *ex post* (achteraf) toezicht van een onafhankelijke instantie mede een bindend oordeel moet kunnen omvatten over de gegeven autorisatie door de minister.[20] In dat geval voldoet het toezichtstelsel als geheel aan de eisen van het EVRM.
- Verder wijzen studies en rapporten op het voordeel van een mengvorm van bestuurlijk-politieke autorisatie gekoppeld aan onafhankelijk bindend *ex post* toezicht dat kan plaatsvinden gedurende de operaties van inlichtingen- en veiligheidsdiensten. De gedachte daarbij is dat de bindende rechtmatigheidsoordelen van een toezichthouder uiteindelijk zullen doorwerken in de bestuurlijk-politieke *ex ante* autorisatie.[21]

Ontwikkeling in Nederland

In Nederland is men zoekende naar de wijze waarop het toezicht op de inlichtingen- en veiligheidsdiensten dient te worden vormgegeven.

Recent stelt het Instituut voor informatierecht van de Universiteit van Amsterdam als één van tien waarborgen dat toezicht op de inlichtingen- en veiligheidsdiensten onafhankelijk dient te zijn en dat rechterlijke controle de beste waarborg voor onafhankelijkheid biedt. Vanuit dat oogpunt wordt rechterlijke controle op de inzet van bijzondere bevoegdheden wenselijk geacht.[22] Echter, het rapport stelt verder als waarborg dat toezicht voorafgaand aan de inzet van bijzondere bevoegdheden essentieel is, maar dat dit niet per definitie door een rechter hoeft te worden uitgevoerd. Als een alternatief voor *ex ante* (vooraf) rechterlijke toetsing wordt een systeem gezien van ministeriële goedkeuring gekoppeld aan direct bindend rechtmatigheidstoezicht door een onafhankelijke gespecialiseerde commissie, aangevuld met *ex post* (achteraf) doelmatigheidstoezicht door het parlement en klachtbehandeling door een onafhankelijke instantie.[23]

---

onderzoek), 30, derde en zesde lid (verkennen van en binnendringen in geautomatiseerde werken; opleggen medewerkingsplicht bij ontsleuteling), 32, tweede lid (gericht afluisteren), 33, tweede lid (interceptie in bulk), 34, vierde lid (onderzoek aan in bulk geïntercepteerde gegevens), 35, tweede en vierde lid (selectie; metadata-analyse), 37, tweede lid (opleggen medewerkingsplicht aan aanbieder van communicatiedienst in het kader van toepassing artikel 33), 38, tweede lid (opleggen verplichting aan aanbieder van communicatiedienst tot verstrekken opgeslagen telecommunicatie) en 41, tweede lid (opleggen medewerkingsplicht bij ontsleuteling).

[20] Het mensenrechtenkader voor het Nederlandse stelsel van toezicht op de inlichtingen- en veiligheidsdiensten, J.P. Loof, J. Uzman, T. Barkhuysen, A.C. Buyse, J.H. Gerards & R.A. Lawson, augustus 2015, p. III, 18, te raadplegen via www.ctivd.nl.

[21] *Ibidem*, p. III.

[22] *Ten Standards for Oversight and Transparency of National Intelligence Services*, Institute for Information Law, University of Amsterdam, 2015, p. i, 36

[23] *Ibidem*, p. 37.

Hiermee hangt samen de ontwikkeling met betrekking tot de bescherming van het verschoningsrecht in Nederland. In navolging van de uitspraak van het EHRM in de *Telegraaf*-zaak (2012), is een tijdelijke voorziening getroffen voor de inzet van bijzondere bevoegdheden tegen journalisten ter bescherming van hun brongeheim en tegelijkertijd is een apart concept-wetsvoorstel ingediend. De kern van de wettelijke regeling is dat voordat bijzondere bevoegdheden mogen worden ingezet, rechterlijke toestemming benodigd is. Dit heeft ook zijn weerslag gekregen in het concept-wetsvoorstel Wiv 20XX (artikel 24 lid 4). Momenteel lopen er gerechtelijke procedures waarin de advocatuur een vergelijkbare wettelijke voorziening vraagt. In juli 2015 heeft de rechtbank Den Haag in kort geding, onder verwijzing naar de overwegingen van het EHRM in de Telegraaf-zaak, overwogen dat onafhankelijk toezicht op de uitoefening van bijzondere bevoegdheden tegen advocaten zeer wenselijk is, waarbij het toezichthoudende orgaan onder meer de bevoegdheid moet hebben de uitoefening van die bevoegdheden tegen te gaan of te beëindigen. De rechter overweegt dat uit de jurisprudentie van het EHRM kan worden opgemaakt dat de waarborg tegen misbruik van bevoegdheden niet noodzakelijkerwijs moet bestaan uit een preventieve rechterlijke toets. Er kan ook gedacht worden aan een controlerend orgaan dat de bevoegdheid heeft om het afluisteren te stoppen of de opbrengsten ervan te vernietigen. De rechtbank overweegt dat de onafhankelijke toets, die de staat binnen zes maanden dient in te voeren, niet in alle gevallen voorafgaand aan de inzet van bijzondere bevoegdheden hoeft plaats te vinden. Zeker bij indirect tappen zal immers niet in alle gevallen vooraf duidelijk zijn dat de verkregen informatie mogelijk onder het verschoningsrecht valt. De rechtbank benadrukt dat de onafhankelijkheid van de CTIVD in artikel 65 Wiv 2002 voldoende is geborgd, maar laat de keuze van maatregelen in beginsel aan de staat.[24] Er is hoger beroep ingesteld.

Aandachtspunten

De CTIVD onderschrijft de in het concept-wetsvoorstel neergelegde waarborg van toestemmingsverlening door de minister voor de inzet van bepaalde bijzondere bevoegdheden. Hierbij onderkent de CTIVD overigens dat op dit punt alleen sprake kan zijn van een waarborg indien het vereiste van ministeriële toestemming niet in zoveel gevallen wordt gesteld, dat een aanvraag vooral een administratieve invuloefening voor de diensten wordt en de inhoudelijke toets van de minister aan waarde verliest. Hierbij is het van belang dat sprake is van duidelijke toetsbare elementen, die de noodzakelijkheid, proportionaliteit en subsidiariteit van de inzet van de bevoegdheid inzichtelijk maken.

De CTIVD vindt het in de eerste plaats op de weg van de ministers liggen de politiek-bestuurlijke, strategische, en juridische afwegingen omtrent bedreigingen van de nationale veiligheid, die inherent zijn aan de inzet van bijzondere bevoegdheden, te maken.[25] Wel is van belang dat in aanvulling hierop (direct) bindend, onafhankelijk toezicht op de rechtmatigheid van de besluitvorming van de minister plaatsvindt. De CTIVD acht het dan ook van belang dat eerst de minister de ruimte krijgt om invulling te geven aan de hem toekomende politieke verantwoordelijkheid.

Onbegrensde handhaving van politieke verantwoordelijkheid is echter niet aan de orde. De samenleving vraagt om een juiste balans, op grondslag van een onafhankelijke toetsing, tussen bescherming van de burgers en de samenleving tegen bedreigingen van de nationale veiligheid en bescherming van de privacy en andere mensenrechten. En daarmee van behoud van het publiek vertrouwen in het werk van de inlichtingen- en veiligheidsdiensten.

---

[24] Rechtbank Den Haag, 1 juli 2015, ECLI:NL:RBDHA:2015:7436, r.o. 4.10, 4.11 en 4.14.

[25] Ook de jurisprudentie van het EHRM biedt steun voor deze lijn. Bij de beoordeling of een bepaalde situatie valt aan te merken als een 'noodtoestand die het land bedreigt' in de zin van artikel 15 EVRM, in welk geval staten bepaalde verdragsverplichtingen mogen opschorten, laat het EHRM staten een grote beoordelingsruimte (*margin of appreciation*), omdat deze afweging beter te maken is door nationale politieke organen dan door een (internationale) rechter; zie *Het mensenrechtenkader voor het Nederlandse stelsel van toezicht op de inlichtingen- en veiligheidsdiensten*, J.P. Loof, J. Uzman, T. Barkhuysen, A.C. Buyse, J.H. Gerards & R.A. Lawson, augustus 2015, p. 18, te raadplegen via www.ctivd.nl.

De CTIVD acht dan ook van essentieel belang dat op de ministeriële lastgeving toezicht wordt uitgeoefend door een onafhankelijke (externe) instantie. Ook het EHRM benadrukt het belang van onafhankelijk *ex post* toezicht. In de eerste plaats als aanvulling op de onafhankelijke toestemmingsverlening. Dit om te controleren of de uitvoering van de onderzoeks- of interceptiebevoegdheid geschiedt op een manier die binnen de wettelijke, mensenrechtelijke en in de toestemmingsverlening aangegeven grenzen blijft. Echter, als geen toestemmingsverlening door een onafhankelijke instantie plaatsvindt (zoals in het concept-wetsvoorstel aan de orde is), dan dient het *ex post* toezicht ook een bindend oordeel over de rechtmatigheid van de verleende toestemming te omvatten.

De CTIVD leidt uit het Europees en internationaal mensenrechtelijk kader af dat onafhankelijke toestemmingsverlening geen strikt vereiste is voor mensenrechtenconformiteit, indien er binnen het gehele stelsel sprake is van voldoende effectieve waarborgen, zoals de mogelijkheid om in te grijpen en opbrengst te laten vernietigen.[26] Daarvan is in het huidige systeem onder de Wiv 2002 en in het voorgestelde stelsel geen sprake. Dit zou echter met de invoering van bindende rechtmatigheidsoordelen gerealiseerd worden. Hier is de CTIVD in het eerste onderdeel van deze reactie reeds uitvoerig op in gegaan.

In aansluiting op het voorgaande vindt de CTIVD het van belang enkele kanttekeningen te plaatsen bij de in met name de wetenschapsliteratuur maar ook elders lopende discussies over het verdelen van het toezicht over enerzijds preventieve of *ex ante* toetsing (door een rechter) en anderzijds *ex post* toetsing (door de CTIVD).

De combinatie van toezicht *ex ante* (toestemming) en *ex post* (uitvoering) bij verschillende instanties kan tot inhoudelijke problemen leiden. Dit doet zich bijvoorbeeld voor bij de beoordeling van verlengingen van de inzet van bijzondere bevoegdheden. Deze beoordeling is niet een zuiver juridische die vooraf aan de hand van de aanvraag (last) kan worden gemaakt. Ook de opbrengst van het middel moet meegewogen worden. Een andere situatie betreft het indirect tappen van advocaten.
Dit houdt in dat de tap is ingezet op een target, maar dat bij de geïntercepteerde communicatie ook communicatie van het target met zijn advocaat zit. Zeker bij indirect tappen zal niet in alle gevallen vooraf duidelijk zijn dat de verkregen informatie mogelijk onder het verschoningsrecht valt. Inzicht hierin vereist toegang tot alle informatie bij de diensten. De voorbeelden illustreren dat effectief toezicht meer behelst dan een toetsing van aangeleverde aanvragen (lasten). Niet alleen is inzicht nodig in de achterliggende documenten, ook gesprekken en veldonderzoek kunnen benodigd zijn om het beeld te complementeren.

De CTIVD benadrukt verder nog dat het weinig wenselijk is naast de reeds bestaande toezichthouder andere instanties te creëren met vergaande toegang tot staatsgeheim materiaal en onderzoeksbevoegdheden bij de inlichtingen- en veiligheidsdiensten. Bovendien vergt het opbouwen van expertise en kennis van het werkterrein van de inlichtingen- en veiligheidsdiensten om een juiste beoordeling te kunnen maken die recht doet aan de belangen van de nationale veiligheid en van individuen, een lange adem. De Venice Commission van de Raad van Europa komt ook tot deze conclusie in haar rapport uit 2007.[27] De CTIVD onderschrijft dit vanuit haar eigen ervaring. Dit pleit ervoor aansluiting te zoeken bij het rechtmatigheidstoezicht van de CTIVD die als gespecialiseerde toezichthouder sinds de oprichting in 2002 bouwt aan haar expertise en ervaring op het gebied van inlichtingen- en veiligheid.

---

[26] Het mensenrechtenkader voor het Nederlandse stelsel van toezicht op de inlichtingen- en veiligheidsdiensten, J.P. Loof, J. Uzman, T. Barkhuysen, A.C. Buyse, J.H. Gerards & R.A. Lawson, augustus 2015, p. 18, te raadplegen via www.ctivd.nl.

[27] European Commission for Democracy through Law (Venice Commission), *Report on the Democratic Oversight of the Security Services*, adopted at its 71st Plenary Session, CDL-AD(2007)016, Strasbourg 11 June 2007, para. 87, p. 19.

De CTIVD wijst erop dat haar *ex post* toezicht 'onmiddellijk' of direct toezicht op de toestemmingsverlening kan inhouden. Het moment van toezicht kan immers plaatsvinden direct na een verleende toestemming, lopende een operatie en na beëindiging van bepaalde werkzaamheden. De bindende kracht van een oordeel over de rechtmatigheid van de toestemming waarborgt bovendien dat dwingend kan worden ingegrepen.

Een ander punt dat aandacht verdient is dat met bindend *ex post* rechtmatigheidstoezicht op de verleende toestemming de ministeriële verantwoordelijkheid voor en aanspreekbaarheid van de ministers op het (beleidsmatig) handelen van de diensten, met name vanuit het parlement, behouden blijft. Anders dan de regering stelt[28], neemt de externe instantie bij een dergelijke toetsing, die vanuit het oogpunt van effectiviteit van het toezicht dient te kunnen resulteren in een bindend oordeel, niet de verantwoordelijkheid voor de inzet van de bevoegdheid over en blijft de ministeriële verantwoordelijkheid voor het handelen van de diensten richting het parlement gehandhaafd. Rechtmatigheidstoezicht, zoals dat van de CTIVD, richt zich op een juridische beoordeling van de autorisatie en de uitvoering van bijzondere bevoegdheden en niet op de doelmatigheid of doeltreffendheid van het gevoerde beleid en de uitvoering ervan. Het toetsingskader wordt ontleend aan de eisen uit de Wiv, die voortvloeien uit het EVRM, namelijk of de inzet van de bijzondere bevoegdheid waarmee inbreuk wordt gemaakt op de grondrechten van burgers voldoet aan de vereisten van noodzakelijkheid, proportionaliteit en subsidiariteit. Er zijn verschillende voorbeelden waar een minister in de uitvoering van zijn beleid kan worden begrensd door oordelen van externe onafhankelijke, niet-rechterlijke, instanties, maar in de richting van het parlement geheel verantwoordelijk blijft voor de uitvoering van zijn beleid. Ter illustratie kan gewezen worden op de Raad voor Strafrechtstoepassing en de Jeugdbescherming (RSJ). De RSJ behoort niet tot de rechterlijke macht, maar heeft tot taak door advies en bindende beslissingen op onafhankelijke wijze er op toe te zien dat de overheid in de beleidsontwikkeling en de uitvoering van de vrijheidsbenemende en vrijheidsbeperkende sancties en jeugdbeschermingsmaatregelen op een juridisch correcte wijze en in overeenstemming met beginselen van goede bejegening te werk gaat.

Advies

De CTIVD ziet grote waarde in de combinatie van ministeriële toestemming voor de inzet van bijzondere bevoegdheden en onafhankelijk *ex post* bindend toezicht op de verleende toestemming van de minister, in ieder geval voor de meest inbreukmakende bevoegdheden, en op de uitvoering van de operaties.

De wijze waarop het rechtmatigheidstoezicht van de CTIVD in het concept-wetsvoorstel beoogt te worden versterkt, is ontoereikend. Hiermee wordt niet voldaan aan de vereisten die onder meer het EHRM stelt aan effectief toezicht. Hiervoor is bindende kracht van de rechtmatigheidsoordelen noodzakelijk.

Hoewel het toezicht van de CTIVD formeel gezien een *ex post* karakter heeft, zal het in de praktijk een direct karakter hebben. Dit betekent dat het toezicht direct na de toestemmingsverlening door de minister wordt uitgevoerd. De bindende kracht van het rechtmatigheidsoordeel waarborgt bovendien dat dwingend ingegrepen kan worden, met als gevolg dat in een voorkomend geval eventueel reeds verkregen opbrengst vernietigd dient te worden.

[28] Kabinetsreactie op het evaluatierapport van de commissie Dessens, *Kamerstukken II*, 2013/2014, 33 820, nr. 2.

1.3 Institutionele scheiding CTIVD

[Artikel 85; p. 159-161 MvT]

Concept-wetsvoorstel

In het concept-wetsvoorstel wordt de CTIVD als zelfstandige onafhankelijk klachtinstantie gepositioneerd die bindende oordelen voor de betrokken minister kan geven. Ook wordt de CTIVD belast met de behandeling van meldingen in verband met vermoede misstanden (klokkenluidersregeling; artikelen 114 e.v.). De CTIVD voert daarnaast het reeds bestaande rechtmatigheidstoezicht op de diensten uit. In het licht van het vereiste van onbevooroordeelde oordeelsvorming, zowel in de uitoefening van het rechtmatigheidstoezicht als in de klachtbehandeling en de behandeling van vermoedens van misstanden, heeft de regering besloten dat voorzien dient te worden in een functionele, personele en organisatorische scheiding om de noodzakelijke onbevooroordeeldheid te kunnen waarborgen. De regering acht het van essentieel belang dat voorkomen wordt dat leden van de CTIVD die in het kader van het rechtmatigheidstoezicht over een bepaalde kwestie hebben geoordeeld, over diezelfde kwestie tevens oordelen in geval van een ingediende klacht of een vermoeden van een misstand. Dat het oordeel van de CTIVD in rechtmatigheidstoezicht in het wetsvoorstel geen bindend karakter krijgt, doet aan dit belang niet af. In eerdere discussies over de wenselijkheid van het verenigen van (externe) klachtbehandeling en rechtmatigheidstoezicht in de CTIVD is als probleem naar voren gebracht dat een toezichthouder die klachten over de diensten behandelt, strikt gesproken ook klachten over zichzelf afdoet. Indien de toezichthouder in één van zijn functies bindende oordelen kan geven, wordt deze onwenselijke situatie nog versterkt. In het wetsvoorstel wordt daarom voorzien in een aparte klachtenafdeling binnen de CTIVD. Bij deze afdeling wordt ook de klokkenluidersregeling onder gebracht. Op deze wijze wordt gehandeld in lijn met de jurisprudentie van het EHRM. Naast de afdeling klachtbehandeling (en misstanden) bestaat de CTIVD verder uit een afdeling toezicht. De leden van de CTIVD (vier in totaal) zijn verdeeld over de afdelingen. Ieder lid kan slechts deel uitmaken van een afdeling. Ook bij de inrichting van het ondersteunende secretariaat dient een personele, functionele en organisatorische scheiding plaats te vinden.

Aandachtspunten

De CTIVD onderschrijft het belang van publiek vertrouwen in de onbevooroordeelde afhandeling van klachten over de inlichtingen- en veiligheidsdiensten. Artikel 13 EVRM vereist een effectief rechtsmiddel op het gebied van klachtbehandeling over inlichtingen- en veiligheidsdiensten. Hieronder wordt onder meer verstaan dat de beoordeling van klachten van burgers geschiedt door een onafhankelijke en onpartijdige instantie.

Het concept-wetsvoorstel stelt voor de externe klachtprocedure bij de CTIVD onder te brengen. Hiervoor dient een aparte afdeling te worden opgericht. Verder dient binnen de CTIVD sprake te zijn van een strikte functionele, personele en organisatorische scheiding tussen toezicht en klachtbehandeling. Het is echter de vraag of het concept-wetsvoorstel hiermee op afdoende wijze een oplossing biedt om een schijn van partijdigheid te voorkomen. Feit blijft immers dat de externe klachtbehandeling plaatsvindt door de CTIVD. Dezelfde instantie die ook verantwoordelijk is voor het rechtmatigheidstoezicht op de inlichtingen- en veiligheidsdiensten.

De CTIVD wijst erop dat er op zichzelf goede argumenten zijn om juist klachtbehandeling en toezicht op de inlichtingen- en veiligheidsdiensten integraal bij hetzelfde orgaan samen te brengen. Deze meerwaarde is onder meer gelegen in het benutten van de reeds bestaande kennis en ervaring met de AIVD en de MIVD.

Hierbij is ook van belang dat het in het Europese en internationale recht geenszins een uitgemaakte zaak is of het verenigen in dezelfde instantie van de functies van klachtbehandeling en toezicht op inlichtingen- en veiligheidsdiensten aanleiding geeft tot een schijn van partijdigheid die een institutionele scheiding vereist.[29] De CTIVD vindt dan ook dat in het concept-wetsvoorstel deze problematiek te zwaar wordt aangezet.

Met de voorgestelde functionele, personele en organisatorische scheiding tussen klachtbehandeling en toezicht wordt in het geheel niet geprofiteerd van de meerwaarde van het onderbrengen van beide functies bij de CTIVD. In feite creëert het concept-wetsvoorstel twee afzonderlijke CTIVD's die behalve een gedeelde naam verder niets met elkaar van doen (mogen) hebben. Dan rijst de vraag ook of het in dat geval niet beter zou zijn deze functie bij een andere instantie onder te brengen.

De CTIVD ziet een duidelijke meerwaarde in het onderbrengen van klachtbehandeling en toezicht bij hetzelfde orgaan, maar dan zonder functionele, personele en organisatorische scheiding. De CTIVD wijst erop dat naar haar inschatting de hoeveelheid klachten die zien op een eerdere beoordeling van een lastgeving bescheiden zal zijn. De praktijk laat zien dat klachten vaak betrekking hebben op andere kwesties, zoals de uitvoering of de duur van veiligheidsonderzoeken, bejegening, kwesties rondom nakoming van afspraken, uitvoering van de zorgplicht, het uitbrengen van ambtsberichten en samenwerking met buitenlandse diensten. Ook een samenloop van een klacht met eerder verricht onderzoek dat heeft geresulteerd in een toezichtrapport zal naar verwachting bescheiden van aard zijn. De kans dat het eerdere onderzoek als zodanig betrekking had op de klager in kwestie, is dus gering. De inrichting van een goede interne klachtprocedure onder verantwoordelijkheid van de betrokken minister zal bovendien naar verwachting het aantal klachten dat daarna wordt ingediend bij de CTIVD verder beperken.

Voorgaande laat onverlet dat de CTIVD zich rekenschap geeft van het belang van publiek vertrouwen in de onbevooroordeelde afhandeling van klachten. Hieraan kan voldoende worden tegemoet gekomen door enkele plaatsvervangende commissieleden aan te stellen, voor het geval een klacht een onderwerp betreft waarover al eerder een (bindend) rechtmatigheidsoordeel is uitgesproken. Op deze wijze is een onbevooroordeelde besluitvorming gewaarborgd binnen de CTIVD, zonder dat tot een ingrijpende en onwenselijke organisatorische scheiding dient te worden overgegaan. Hierbij vindt de CTIVD nog van essentieel belang dat alleen de commissieleden inhoudelijke beslissingsbevoegdheid hebben. Daarom dient op dit punt een voorziening te worden getroffen om een eventuele schijn van partijdigheid te voorkomen. Deze noodzaak bestaat daarentegen niet met betrekking tot het secretariaat waarvan de onderzoekers deel uit maken. Zij waarborgen de benodigde continuïteit van expertise binnen de organisatie.

[29] *Het mensenrechtenkader voor het Nederlandse stelsel van toezicht op de inlichtingen- en veiligheidsdiensten*, J.P. Loof, J. Uzman, T. Barkhuysen, A.C. Buyse, J.H. Gerards & R.A. Lawson, augustus 2015, p. 37-44, te raadplegen via www.ctivd.nl.

In aanvulling op de voorziening van (enkele vaste) onafhankelijke plaatsvervangende commissieleden, hecht de CTIVD aan de opstelling van een protocol over de afhandeling van klachten. Een beslissing over het al dan niet aanwezig zijn van samenval met een eerdere beslissing in het kader van de toezichtstaak, wordt, voor aanvang van de klachtbehandeling, in alle gevallen gemotiveerd aan de burger medegedeeld. Ook hecht de CTIVD aan de invoering van een 'wrakings-' en herzieningsprocedure in het geval de klager vooraf dan wel achteraf van mening is dat er wel sprake is van een samenloop met een eerdere beslissing/onderzoek in het toezicht ('zelfde rechtsvraag') en de CTIVD heeft geoordeeld dat hiervan geen sprake is. De kwestie wordt dan ter beoordeling voorgelegd aan de plaatsvervangende commissieleden. Afhankelijk van hun oordeel zal de klacht door de plaatsvervangende commissieleden (opnieuw) worden behandeld en beoordeeld. De Nationale ombudsman kent een vergelijkbare (herzienings)procedure wanneer een klager het niet eens is met het oordeel om de klacht niet in behandeling te nemen of met het oordeel ten gronde.[30]

De CTIVD is van mening dat dit voorstel ook kan gelden voor de regeling van vermoede misstanden die in het concept-wetsvoorstel is ondergebracht bij de afdeling klachtbehandeling (artikel 114 en verder juncto artikel 85 lid 4).

Advies
De CTIVD adviseert de taken op het gebied van toezicht, klachtbehandeling en misstanden zonder de voorgestelde functionele, personele en organisatorische scheiding in haar organisatie onder te brengen. Op deze wijze wordt de meerwaarde van het verenigen van deze functies bij de CTIVD, namelijk de opgebouwde expertise met de diensten, volledig benut. Het belang van onbevooroordeelde oordeelsvorming wordt gewaarborgd door de aanstelling van enkele onafhankelijke plaatsvervangende commissieleden. Ook protocollering en de invoering van een 'wrakings'- en herzieningsprocedure draagt hieraan in voldoende mate bij.

1.4 Enkele bevoegdheden CTIVD

[artikelen 113 lid 3 en 120 lid 5; p. 165, 169 MvT]

1.4.1 Beoordeling staatsgeheime karakter van informatie

Concept-wetsvoorstel
Artikel 113 van het concept-wetsvoorstel regelt de taak van de CTIVD/afdeling klachtbehandeling bij de beoordeling van klachten. Artikel 120 doet hetzelfde voor de taak van de CTIVD/afdeling klachtbehandeling bij de beoordeling van vermeende misstanden.

[30] www.nationaleombudsman.nl (bij klacht over de nationale ombudsman).

Aandachtspunten

Nu de CTIVD/klachtafdeling in het concept-wetsvoorstel bindende oordelen in klachtzaken gaat geven en daarmee kan worden beschouwd als een rechterlijk college in de zin van de jurisprudentie van het EHRM, ligt het op haar weg zelf te kunnen beslissen over de status van geheimhouding van tekst(onderdelen) in haar oordelen. In de memorie van toelichting bij artikel 113 lijkt het erop dat die verantwoordelijkheid ook bij de CTIVD/klachtafdeling wordt gelegd in met name het derde lid van artikel 113. De memorie van toelichting zegt daarover: "De uitkomst van het onderzoek door de afdeling klachtbehandeling wordt zowel aan klager als aan de betrokken minister medegedeeld. Bij de mededeling van haar oordeel aan klager zal de afdeling klachtbehandeling deze, voor zover de veiligheid dan wel andere gewichtige belangen van de staat zich daartegen niet verzetten, met redenen dienen te omkleden (artikel 113, derde lid, van het concept-wetsvoorstel). Dat legt op de afdeling klachtbehandeling een bijzondere verantwoordelijkheid, nu zij derhalve ervoor dient te waken dat door haar staatsgeheime informatie wordt geopenbaard."[31] De CTIVD kan zich vinden in deze bevoegdheid. Wel is zij van oordeel dat de tekst van artikel 113 derde lid ("de afdeling klachtbehandeling deelt haar oordeel voor zover de veiligheid dan wel andere gewichtige belangen van de staat zich daartegen niet verzetten, met redenen omkleed aan klager mede") op dit punt duidelijker moet worden geformuleerd in de zin dat de CTIVD/afdeling zelf het besluit over de al of niet geheimhouding van informatie neemt.

Hetzelfde speelt in artikel 120 derde lid (oordelen over misstanden). Deze bepaling is op gelijke wijze geformuleerd als artikel 113 lid 3. Uit het artikel en de memorie van toelichting kan worden afgeleid dat de CTIVD/klachtafdeling zelf over de openbaarmaking en beoordeling van het staatsgeheime karakter van materiaal gaat. In de memorie van toelichting staat: "De afdeling klachtbehandeling deelt vervolgens de melder haar oordeel schriftelijk en, voor zover de veiligheid of andere gewichtige belangen van de staat er niet tegen verzetten, gemotiveerd mede." Vervolgens dient de minister het oordeel samen met zijn reactie daarop aan het parlement/CIVD te sturen. Ook artikel 120 lid 3 dient duidelijker te vermelden dat de CTIVD beslist welke informatie openbaar of geheim moet blijven in haar oordelen.

Indien de rechtmatigheidsoordelen van de CTIVD bindende kracht krijgen dan dient in een vergelijkbare constructie voor deze oordelen te worden voorzien.

Advies

De CTIVD adviseert in de formulering van artikel 113 derde lid (oordelen over klachten) te verduidelijken in de zin dat de CTIVD het besluit neemt over de al of niet geheimhouding van informatie. Hetzelfde geldt voor artikel 120 lid 3 (oordelen over misstanden).

[31] Memorie van toelichting, p. 165.

1.4.2 Geheimhoudingsplicht oud-medewerkers

[artikelen 95 lid 1 en 125 lid 3]

Concept-wetsvoorstel
Een ieder die betrokken is bij de uitvoering van de Wiv is verplicht de CTIVD alle inlichtingen te verstrekken die zij voor een goede uitoefening van haar taak noodzakelijk acht (artikel 95 lid 1). De medewerkers van de diensten kunnen dus niet hun geheimhoudingsplicht inroepen tegenover de CTIVD. Het spreekt vanzelf dat deze bepaling cruciaal is voor het functioneren van het toezicht. Deze uitzondering op de geheimhoudingsplicht geldt echter niet voor personen die in het verleden betrokken zijn geweest bij de uitvoering van de Wiv. Oud-medewerkers van de diensten mogen alleen een verklaring afleggen aan de CTIVD over staatsgeheime zaken als zij door de minister van BZK dan wel Defensie en de minister van Veiligheid en Justitie gezamenlijk ontheven zijn van hun geheimhoudingsplicht (artikel 125, leden 2 en 3).

Aandachtspunten
Het kan naar het oordeel van de CTIVD niet de bedoeling zijn in het concept-wetsvoorstel oud-medewerkers uit te zonderen van een mededelingsplicht aan de CTIVD. De ervaring leert dat juist oud-medewerkers een belangrijke rol kunnen spelen in onderzoeken van de CTIVD. Bijvoorbeeld als tijdens een onderzoek blijkt dat een bepaalde afweging niet schriftelijk is vastgelegd, kan het nodig zijn om te spreken met degene die verantwoordelijk was voor de besluitvorming. Het levert een onwenselijke situatie op als deze persoon alleen met de CTIVD mag spreken over staatsgeheime zaken als hij ontheven is van zijn geheimhoudingsplicht door de minister die verantwoordelijk is voor de instantie waarop toezicht wordt gehouden. Dit doet volgens de CTIVD afbreuk aan haar onafhankelijke positie.

Overigens speelt dit probleem vooral bij de behandeling van klachten. Met name bij klachten is het vaak nodig om het handelen van medewerkers in een bepaalde specifieke zaak in het verleden te reconstrueren. De CTIVD verwacht dat het onderzoeken van vermeende misstanden hiermee vergelijkbaar zal zijn, zij het dat dan een nog groter belang bestaat om het onderzoek in volledige onafhankelijkheid van de onderzochte instantie (en de voor die instantie verantwoordelijke minister) uit te voeren.

Advies
De CTIVD adviseert aan artikel 95 lid 1 toe te voegen dat ook een ieder die betrokken is geweest bij de uitvoering van de Wiv verplicht is inlichtingen te verschaffen aan de CTIVD.

1.5 Gevolgen voor de organisatie en werkwijze van de CTIVD

Concept-wetsvoorstel
De wijziging van de Wiv 2002 zal leiden tot uitbreiding van de bevoegdheden van de inlichtingen- en veiligheidsdiensten. Deze uitbreiding vindt plaats onder gelijktijdige aanscherping van bestaande en introductie van nieuwe waarborgen en zal leiden tot geïntensiveerd toezicht.

Aandachtspunten

Er zal niet alleen sprake zijn van meer en grotere gegevensbestanden, maar ook van toenemende geautomatiseerde ontsluiting en analyse van die bestanden. Kern van toezicht is het vermogen tot volledige controleerbaarheid: de mogelijkheden van de CTIVD om in het licht van deze ontwikkelingen zowel kwantitatief als kwalitatief goed toezicht te kunnen blijven uitoefenen, vergen naast de tot op heden gehanteerde toezichtsvormen ook vormen van geautomatiseerd toezicht. Naar de mogelijkheden van deze vormen van toezicht verricht de CTIVD momenteel onderzoek.

De belangrijkste randvoorwaarden hierbij zijn:

- een vastgestelde administratieve organisatie van de diensten, inclusief functiescheiding, compartimentering en transparant gegevensbeheer;
- meer (geautomatiseerde) standaard rapportagevormen van de diensten ten behoeve van de toezichthouder;
- onmiddellijke digitale ontsluiting van gegevensbestanden voor toezicht, waaronder ook de daarbij gebruikte software bij de diensten, en een procedure waarbij onmiddellijk actie wordt ondernomen bij de vaststelling van onrechtmatigheden; en tenslotte
- een adequate organisatie en werkwijze van de toezichthouder zelf.

Voor wat betreft dit laatste punt zal aan het bestaande onderzoeksprotocol van de CTIVD moeten worden toegevoegd een gestandaardiseerde controle op lasten en bewaartermijnen en zal het profiel van de leden van de CTIVD en de onderzoekers moeten worden uitgebreid met kennis van data-analyse en van (elementair) gegevensbeheer. De toename van het onderzoeksdomein en -bereik zal moeten leiden tot een kwantitatieve uitbreiding van de inzet van de leden van de CTIVD en van het aantal onderzoekers.

De memorie van toelichting vermeldt in dit verband: “Voorts is een belangrijke voorwaarde voor de modernisering van het interceptiestelsel de intensivering van het toezicht door de Commissie van toezicht betreffende de inlichtingen- en veiligheidsdiensten (CTIVD). De CTIVD zal daarvoor in personele zin worden versterkt. De benodigde middelen voor deze intensivering van de CTIVD zullen worden toegevoegd aan de Rijksbegroting hoofdstuk III, Algemene Zaken.”[32]

Advies

De uitbreiding van bevoegdheden van de AIVD en de MIVD en de mede daaraan gerelateerde sterke toename van de gegevensverwerking, zal de toezichtsfunctie in omvang en intensiteit sterk doen groeien. Dit vraagt om een toename van de capaciteit van de CTIVD op alle niveaus.

[32] Memorie van toelichting, p. 202.

1.6 Conclusie

De vraag die in dit hoofdstuk centraal staat is of de positie van de CTIVD als toezichthouder in het concept-wetsvoorstel voldoende wordt versterkt. Het antwoord op deze vraag luidt dat dit, voor wat betreft het toezicht op de rechtmatigheid van het handelen van de diensten, niet het geval is. De CTIVD krijgt onvoldoende bevoegdheden. De voorgestelde heroverwegingsplicht voor de ministers, met parlementaire controle van de CIVD, biedt hier onvoldoende tegenwicht voor. Het voornaamste gebrek is dat de CTIVD geen bindende rechtmatigheidsoordelen toekomt bij de toetsing van de toestemming en van de uitvoering van de meest inbreukmakende bijzondere bevoegdheden, zoals de afluisterbevoegdheid en de hackbevoegdheid. Een bindend oordeel over de rechtmatigheid houdt in dat de CTIVD dwingend kan ingrijpen, waardoor een onrechtmatige operatie dient te worden beëindigd en onrechtmatig verzamelde gegevens dienen te worden vernietigd.

Bindend rechtmatigheidstoezicht vormt niet alleen een waarborg tegen ongerechtvaardigde inbreuken op de mensenrechten van burgers, het is ook één van de vereisten voor effectief toezicht op grond van Europees en internationaal mensenrechtelijke normen. Dit is des te belangrijker nu het toezicht van de CTIVD in feite een door de burger in te roepen rechtsmiddel tegen de inbreuk op zijn privacy vervangt. Vanwege het heimelijke karakter van bijzondere bevoegdheden zal de burger immers in de regel geen kennis hebben van de activiteiten van de diensten en de inbreuk op zijn privacy. De CTIVD is de enige externe instantie met volledige en zelfstandige onderzoeksbevoegdheden bij de diensten. Hierdoor heeft de CTIVD de mogelijkheid de activiteiten van de diensten daadwerkelijk te toetsen aan de kaders die door de wetgever zijn opgelegd.

Het is van belang te benadrukken dat onafhankelijk rechtmatigheidstoezicht, zoals dat van de CTIVD, zich richt op een juridische beoordeling van de autorisatie en van de uitvoering van bijzondere bevoegdheden en niet op de doelmatigheid of doeltreffendheid van het gevoerde beleid en de uitvoering ervan. Bindend *ex post* rechtmatigheidstoezicht tast de ministeriële verantwoordelijkheid voor en aanspreekbaarheid van de ministers op het (beleidsmatig) handelen van de diensten, met name vanuit het parlement, dan ook niet aan. Ook op andere terreinen kan een minister in de uitvoering van zijn beleid begrensd worden door oordelen van externe onafhankelijke instanties, terwijl hij in de richting van het parlement geheel verantwoordelijk blijft voor de uitvoering van zijn beleid.

De CTIVD adviseert dan ook tot de invoering van een bindend rechtmatigheidsoordeel voor de meest inbreukmakende bijzondere bevoegdheden.

In dit hoofdstuk vraagt de CTIVD ook aandacht voor de voorgestelde institutionele scheiding van de CTIVD die feitelijk resulteert in de oprichting van twee CTIVD's die niets met elkaar van doen mogen hebben. Niet alleen schiet dit het beoogde doel van een onbevooroordeelde oordeelsvorming voorbij, nu de perceptie van partijdigheid niet wordt weggenomen, op deze wijze wordt in het geheel niet geprofiteerd van de meerwaarde van het onderbrengen van de functies van toezicht en klachtbehandeling bij de CTIVD. Dan rijst de vraag of het in dat geval niet beter zou zijn deze functie bij een andere instantie onder te brengen.

De CTIVD ziet een duidelijke meerwaarde in het onderbrengen van klachtbehandeling en toezicht in haar organisatie, maar dan zonder de voorgestelde functionele, personele en organisatorische scheiding. Het belang van publiek vertrouwen en onpartijdigheid kan in voldoende mate gewaarborgd worden door de aanstelling van enkele vaste onafhankelijke plaatsvervangende commissieleden, door protocollering van de procedures en de invoering van een 'wrakings'- en herzieningsprocedure.

2 Waarborgen en voorwaarden voor (effectief) toezicht

2.1 Inleiding

Een voorwaarde voor het kunnen uitoefenen van effectief toezicht is een normenkader met regels die duidelijk en nauwkeurig zijn en waarin wordt gewerkt met begrippen die zo concreet mogelijk zijn. Uiteraard is het niet de bedoeling dat de wet en de memorie van toelichting zodanig gedetailleerd en concreet zijn dat de werkwijzen van de diensten daaruit zonder meer kunnen worden afgeleid. Bovendien moeten de regels ruimte laten voor nieuwe ontwikkelingen. Het moet echter wel inzichtelijk zijn in welke gevallen de diensten een bevoegdheid mogen uitoefenen en wat hierbij de randvoorwaarden zijn. In dit hoofdstuk heeft de CTIVD het volgende onderzocht: **Biedt het concept-wetsvoorstel voldoende houvast voor het uitoefenen van toezicht?**

De volgende onderwerpen komen aan de orde:
- Inzet bijzondere bevoegdheden ter ondersteuning van de taak (hoofdstuk 2.2)
- Onderzoek van communicatie (hoofdstuk 2.3)

De adviezen van de CTIVD zijn in de tekst telkens in een **kader** weergegeven.

2.2 Inzet bijzondere bevoegdheden ter ondersteuning van de taak

[artikel 23 tweede lid; p. 31-32 MvT]

Concept-wetsvoorstel

Het voorgestelde artikel 23 koppelt de uitoefening van bijzondere bevoegdheden aan de goede taakuitvoering van de diensten. Het eerste lid van het artikel geeft aan dat bijzondere bevoegdheden mogen worden ingezet voor zover dit *noodzakelijk* is voor de goede taakuitvoering. Dit artikel is opgenomen in artikel 18 van de huidige Wiv 2002.

Het tweede lid creëert de mogelijkheid voor de diensten bijzondere bevoegdheden in te zetten *ter ondersteuning* van de goede taakuitvoering. Het tweede lid is nieuw opgenomen in het concept-wetsvoorstel. De CTIVD bespreekt hierna enkel het tweede lid van het voorgestelde artikel 23.

Het concept-wetsvoorstel geeft een limitatieve opsomming in welke gevallen bijzondere bevoegdheden mogen worden ingezet ter ondersteuning van de goede taakuitvoering. Ten eerste om te beoordelen of het noodzakelijk is bijzondere veiligheidsmaatregelen te treffen voor medewerkers van een dienst of andere personen die een taak (zullen) vervullen voor de dienst. Ten tweede om te beoordelen of personen, met wier medewerking gegevens worden verzameld, betrouwbaar zijn.

Uit het vijfde lid van voorgesteld artikel 24 volgt dat van een verleende toestemming de CTIVD direct op de hoogte gebracht moet worden.

Aandachtspunten

De CTIVD heeft in verschillende klachtzaken en toezichtsrapporten beschreven dat de Wiv 2002 de mogelijkheid biedt bijzondere bevoegdheden uitsluitend in te zetten indien dit noodzakelijk is voor de goede taakuitvoering. De Wiv 2002 biedt geen ruimte voor de inzet van bijzondere bevoegdheden ter ondersteuning van de goede taakuitvoering. De CTIVD heeft verschillende malen een onrechtmatigheidsoordeel uitgesproken over het inzetten van bijzondere bevoegdheden voor het vaststellen van de betrouwbaarheid van een bron.

Het concept-wetsvoorstel biedt in het tweede lid van artikel 23 in twee expliciet omschreven gevallen de wettelijke grondslag ter ondersteuning van de taak bijzondere bevoegdheden in te zetten. De CTIVD stelt hierna enkele aandachtspunten over de voorgestelde regeling aan de orde. Zij bespreekt eerst haar opmerkingen over onderdeel a van het tweede lid ('onderzoek voor bijzondere veiligheidsmaatregelen'). Daarna gaat zij in op onderdeel b van het tweede lid ('betrouwbaarheidsonderzoek').

Onderzoek voor bijzondere veiligheidsmaatregelen (artikel 23, lid 2, onder a)

Voor de CTIVD is het onvoldoende duidelijk wanneer sprake is van een situatie waarin de veiligheid van een medewerker[33] aanleiding geeft tot de inzet van een bijzondere bevoegdheid. De CTIVD vraagt zich af of de fysieke veiligheid in het geding moet zijn of dat de kans op (ongewenste) onderkenning als medewerker van een dienst al voldoende is. De CTIVD gaat ervan uit dat sprake moet zijn van een dreiging tegen een medewerker van de dienst. Dit blijkt echter niet uit het concept-wetsvoorstel of de memorie van toelichting. Het is de CTIVD daardoor ook niet duidelijk hoe deze dreiging moet worden beoordeeld. Dient sprake te zijn van een concrete dreiging of is een voorstelbare dreiging (bijvoorbeeld gelet op de specifieke targetgroep) al voldoende?

De memorie van toelichting vermeldt slechts één voorbeeld bij deze vorm van ondersteunende inzet van bijzondere bevoegdheden. De situatie wordt geschetst dat een bijzondere bevoegdheid wordt ingezet om het netwerk rond een bron in kaart te brengen. In dit voorbeeld wordt de bijzondere bevoegdheid ingezet tegen de bron. Hiermee kunnen de risico's voor de bron in kaart worden gebracht, aldus de memorie van toelichting. De CTIVD merkt op dat een bron, in meer of mindere mate, altijd risico zal kunnen lopen bij zijn werkzaamheden voor de dienst. Dit risico zal volgens de CTIVD wel moeten worden geconcretiseerd wil deze de inzet van bijzondere bevoegdheden kunnen rechtvaardigen. Het enkele risico op onderkenning van de bron acht de CTIVD in ieder geval daarvoor van onvoldoende gewicht. De CTIVD gaat ervan uit dat kennelijk gedoeld wordt op het heimelijk inzetten van een bijzondere bevoegdheid tegen de bron. De voorgestelde bepaling biedt zoveel ruimte dat deze in feite in iedere situatie waarbij wordt samengewerkt met een bron van toepassing is.

Het is voor de CTIVD niet duidelijk of het concept-wetsvoorstel ook voorziet in de mogelijkheid tot het inzetten van bijzondere bevoegdheden ter beveiliging van een ontmoeting tussen een bron en een medewerker van de AIVD. De hiervoor genoemde aandachtspunten gelden in dit verband ook. Dient sprake te zijn van een concrete gevaarzetting die uitgaat van de ontmoeting, bijvoorbeeld omdat de bron ook aangemerkt kan worden als (gewelddadig) target? Indien dit niet het geval is, wat zijn dan de randvoorwaarden? Het concept-wetsvoorstel biedt hierover geen nadere aanknopingspunten.

Indien de regeling onvoldoende duidelijk is, is het ook slechts in beperkte zin mogelijk hierop toezicht uit te oefenen. Dat maakt de plicht de CTIVD direct te informeren van een verleende toestemming in dat geval van weinig waarde.

---

[33] Waar gesproken wordt over de veiligheid van een medewerker bedoelt de CTIVD ook de veiligheid van andere personen die een taak (zullen) vervullen voor de diensten.

Betrouwbaarheidsonderzoek (artikel 23, lid 2, onder b)
Uit het concept-wetsvoorstel en de memorie van toelichting blijkt volgens de CTIVD onvoldoende in welke gevallen het mogelijk is bijzondere bevoegdheden in te zetten bij een betrouwbaarheidsonderzoek. De memorie van toelichting schetst de situatie waarbij een dienst onderzoek verricht om te controleren of een agent niet ook wordt aangestuurd door een andere inlichtingendienst (een zogenaamde dubbelagent). Het is de CTIVD onduidelijk of de diensten aanwijzingen moeten hebben dat de betrouwbaarheid van een bron in twijfel moet worden getrokken. Indien dit het geval is, vraagt de CTIVD zich af wat de toegevoegde waarde is van het concept-wetsvoorstel. Indien de diensten aanwijzingen hebben dat een persoon (heimelijk) werkzaam is voor een buitenlandse inlichtingendienst, zal het onderzoek naar deze persoon al snel *noodzakelijk* zijn in het kader van de taakuitvoering omdat hij als target aangemerkt kan worden.

Indien het ontbreken van aanwijzingen hiervoor niet in de weg staat aan het inzetten van bijzondere bevoegdheden, betekent dit dat in alle gevallen bijzondere bevoegdheden mogen worden ingezet tegen agenten om het punt van buitenlandse beïnvloeding te onderzoeken. Het concept-wetsvoorstel lijkt dus de ruimte te bieden de betrouwbaarheid van bronnen te onderzoeken ook als de betrouwbaarheid van een bron (nog) niet ter discussie staat. De CTIVD benadrukt dat bronnen van de diensten in beginsel vertrouwen dienen te genieten. Dit uitgangspunt zou ook met het concept-wetsvoorstel overeind moeten blijven.

Aangezien de memorie van toelichting slechts één voorbeeld schetst van een betrouwbaarheids-onderzoek, is het voor de CTIVD onduidelijk in welke andere gevallen een betrouwbaarheidsonderzoek met de inzet van bijzondere bevoegdheden mogelijk wordt geacht. Is een dergelijk onderzoek bijvoorbeeld toegestaan indien de diensten reden hebben te twijfelen aan de door een bron verschafte informatie, bijvoorbeeld omdat de informatie onvolledig of feitelijk onjuist is?

Het direct informeren van de CTIVD van een verleende toestemming voor betrouwbaarheidsonderzoek is van weinig waarde indien de regeling onvoldoende duidelijk is. Hierdoor is het slechts in beperkte zin mogelijk hierop toezicht uit te oefenen.

Advies
De CTIVD adviseert meer duidelijkheid te scheppen over het toepassingsgebied van artikel 23 lid 2 onder a en b en dit aan de hand van concrete voorbeelden toe te lichten.

2.3 Onderzoek van communicatie

[artikelen 31-35 en artikel 47; p. 57-84, 101-103 MvT]

Concept-wetsvoorstel
Paragraaf 3.2.2.7 van het concept-wetsvoorstel gaat over de bijzondere bevoegdheden die de diensten in staat stellen onderzoek van communicatie te verrichten. De belangrijkste wijzigingen ten opzichte van de huidige wettelijke regeling hebben betrekking op de bepalingen over de verwerving en verwerking van telecommunicatie in bulk. In het concept-wetsvoorstel is gekozen voor een techniekonafhankelijke formulering, waardoor de bevoegdheid zich ook uitstrekt tot kabelgebonden telecommunicatie. Het concept-wetsvoorstel introduceert een driefasenmodel en maakt de bevoegdheden die daaronder geschaard worden onderhevig aan ministeriële toestemming.

De CTIVD vindt het, gezien haar toezichthoudende taak, niet op haar weg liggen om ten aanzien van de uitbreiding van bevoegdheden op het terrein van kabelgebonden telecommunicatie een standpunt in te nemen. De CTIVD heeft zich wel de vraag gesteld of de voorgestelde interceptiebevoegdheden voldoende waarborgen kennen tegen ongeoorloofde inbreuken op de persoonlijke levenssfeer en duidelijke aanknopingspunten bevatten voor toezicht. De CTIVD stelt vast dat de beschrijving van het voorgestelde interceptiestelsel in de memorie van toelichting een vereenvoudigde weergave is. De CTIVD neemt in het kader van haar toezicht in de praktijk een complexere werkelijkheid waar, die ook zal gelden voor het voorgestelde interceptiestelsel. Om haar kanttekeningen bij het voorgestelde interceptiestelsel duidelijk voor het voetlicht te kunnen brengen, heeft de CTIVD hier een fictieve casus opgesteld over de werking van de verschillende fasen in het voorgestelde interceptiestelsel. De CTIVD beoogt met deze fictieve casus ook het politieke en maatschappelijke debat te informeren.

De CTIVD bespreekt hierna eerst het driefasenmodel aan de hand van een schema en een fictieve casus.

2.3.1 Toelichting driefasenmodel

De CTIVD ziet het driefasenmodel (d.w.z. verwerving, voorbewerking en (verdere) verwerking) niet als een aan tijd of hoeveelheid gegevens verbonden proces. Het is niet het geval dat een fase pas begint als de voorgaande is doorlopen. Het is ook niet zo dat in iedere opvolgende fase per definitie gewerkt wordt met minder gegevens. In de praktijk gaat het om continue processen die elkaar voortdurend beïnvloeden. Deze processen vinden bovendien grotendeels plaats ten aanzien van dezelfde hoeveelheid verzamelde communicatiegegevens.

De drie fasen corresponderen met de mate van inbreuk op de persoonlijke levenssfeer die aan de orde kan zijn. De bevoegdheden die worden geschaard onder fase 2 zijn over het algemeen minder inbreukmakend dan de bevoegdheden onder fase 3, maar meer inbreukmakend dan de bevoegdheden onder fase 1.

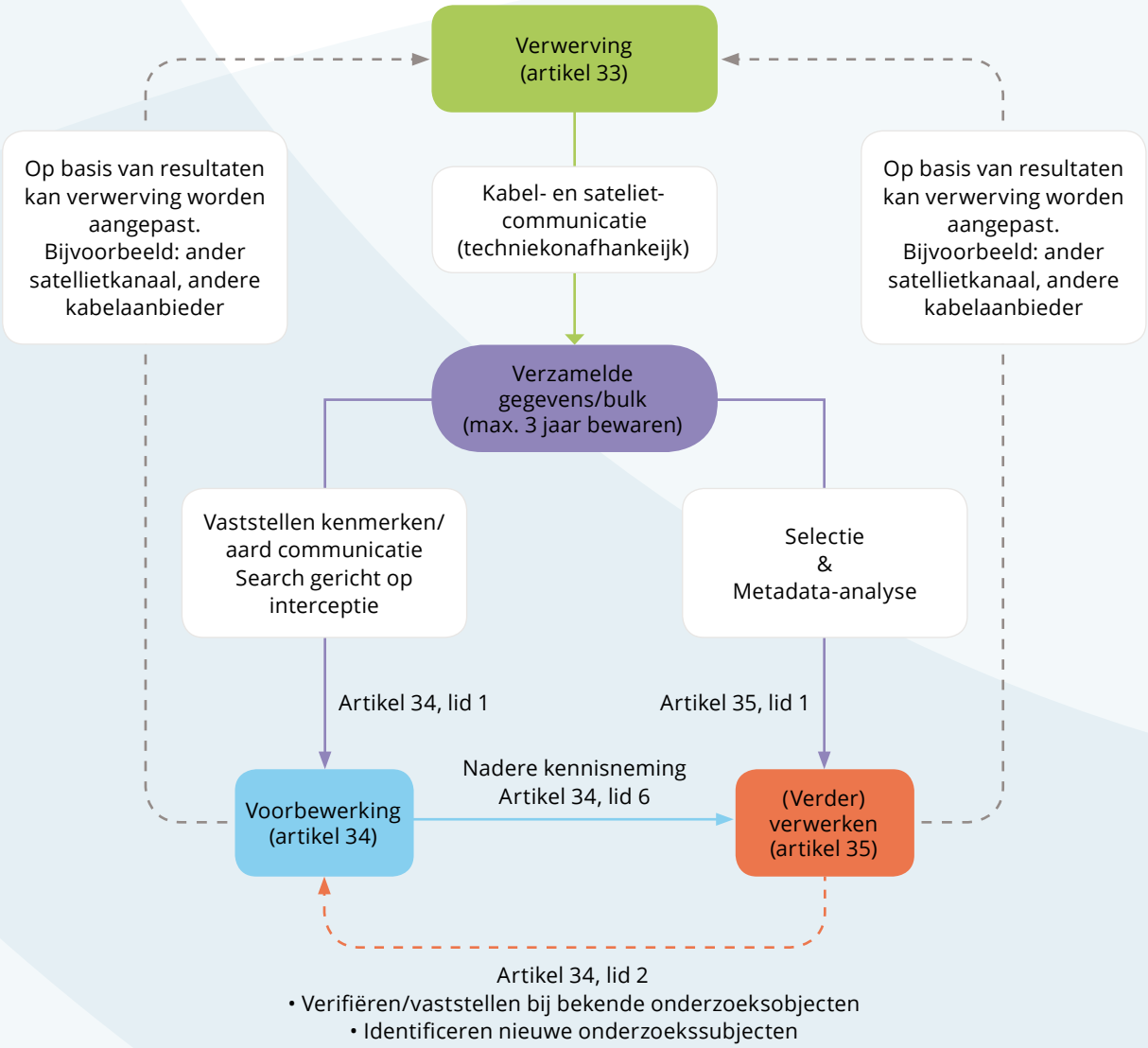
De CTIVD heeft het driefasenmodel hieronder schematisch weergegeven. Zij heeft daarnaast ter verduidelijking van haar standpunt aan de hand van een fictieve casus uiteengezet hoe het driefasenmodel in de praktijk zou kunnen worden gebracht. In de tekst van de fictieve casus en verder in de reactie verwijst de CTIVD telkens naar het onderstaande schema.[34]

De fictieve casus betreft een versimpelde weergave van de werkelijkheid. De casus beschrijft bovendien de situatie van een concreet target waar een bepaalde dreiging vanuit gaat. In veel gevallen, met name bij de inzet van de Nederlandse krijgsmacht bij militaire missies in het buitenland, is echter geen sprake van een concrete persoon of organisatie van wie een dreiging uitgaat.[35] In die gevallen is het bedreigde het uitgangspunt van het onderzoek. Het onderzoek is er dan op gericht mogelijke dreigingen tijdig te onderkennen. Dit maakt het proces minder concreet.

---

[34] De CTIVD heeft door middel van kleurgebruik in het schema en de tekst geprobeerd haar reactie over het nieuwe interceptiestelsel inzichtelijker te maken.

[35] Het gaat hierbij om de begrippen 'threat to the force' (dreigingen gericht tegen Nederlandse of bondgenootschappelijke troepen) en 'threat to the mission' (gevaren voor het behalen van de doelstelling van de militaire missie).



Fictieve casus

Eén van de inlichtingen- en veiligheidsdiensten (IVD) doet onderzoek naar een terroristische groepering (organisatie X). Organisatie X is actief in een bepaald land (land Y). De IVD heeft aanwijzingen dat organisatie X een terroristisch trainingskamp heeft in land Y. In het trainingskamp zouden leden van organisatie X worden voorbereid op het plegen van aanslagen in Europa. Het trainingskamp zou de bijnaam traika hebben. Enkele personen die deel uitmaken van organisatie X zijn bij de IVD bekend. Het gaat om A, B en C. Van deze personen zijn drie telefoonnummers bekend. Uit een andere inlichtingenbron is een aanwijzing gekomen dat organisatie X banden zou hebben met enkele hoge overheidsfunctionarissen van land Z. Organisatie X wordt mogelijk door hen gefinancierd. Het vermoeden bestaat dat er e-mailcontact is geweest tussen leden van organisatie X en enkele hoge overheidsfunctionarissen van land Z.

De IVD heeft de volgende onderzoeksvragen:

- Welke personen maken nog meer deel uit van organisatie X?
- Heeft organisatie X daadwerkelijk een terroristisch trainingskamp in land Y, waar leden worden voorbereid op het plegen van aanslagen in Europa?
- Zijn er banden tussen organisatie X en enkele hoge overheidsfunctionarissen van land Z?

Verwerving (groene blok in schema) en voorbewerking (blauwe blok in schema)

Om de onderzoeksvragen te kunnen beantwoorden wordt het interceptieproces in gang gezet. Allereerst speelt de vraag over welke satellietkanalen en kabels communicatie wordt getransporteerd die voor dit onderzoek relevant is.

De IVD maakt de inschatting dat GSM-verkeer van en naar land Y en internetverkeer tussen land Y en land Z relevante communicatie kan bevatten. De IVD vraagt op basis van artikel 33 van het wetsvoorstel (verwerving) toestemming aan de minister voor het intercepteren van deze communicatie. De toestemming wordt verkregen voor een jaar.

Als de minister toestemming geeft kan weliswaar de communicatie worden verworven, maar het is nog niet duidelijk over welke satellietkanalen en kabels die communicatie wordt getransporteerd. Ook moet, vanwege capacitaire beperkingen, een keuze worden gemaakt. Zo kan het bijvoorbeeld zijn dat bij de IVD bekend is dat over twee satellietkanalen GSM-verkeer vanuit land Y verloopt, maar dat er slechts capaciteit is om één van deze satellietkanalen te intercepteren.

De IVD heeft de bevoegdheid technisch en inhoudelijk onderzoek aan de communicatie te verrichten (voorbewerking). Het gaat hier om zowel de technische analyse (artikel 33 concept-wetsvoorstel) als om search gericht op interceptie (artikel 34 lid 1 concept-wetsvoorstel). Dit technische en inhoudelijke onderzoek aan de communicatie is ervoor bedoeld zo goed mogelijk te bepalen over welke satellietkanalen en kabels communicatie wordt getransporteerd die relevant is voor het onderzoek. Het technisch en inhoudelijk onderzoek aan de communicatie kan bijvoorbeeld antwoord geven op de volgende vragen:

- Wat is de aard van het verkeer (GSM, radio, internet, tv-signalen etc.)?
- Wat is de soort verkeer (spraak, chat, fax etc.)?
- Waar gaat de communicatie naar toe/waar komt het vandaan?
- Welke partijen communiceren er? Is het militair verkeer?
- Komen de in het onderzoek bekende technische kenmerken voor (de in de casus vermelde telefoonnummers van A, B en C)?

Voor het verrichten van het onderzoek aan de communicatie moet gemotiveerd toestemming worden gevraagd aan de minister (artikel 34 lid 1 concept-wetsvoorstel). In het schema is dit de **linker paarse lijn**. De toestemming wordt verkregen voor een jaar. Het verzoek om toestemming voor het onderzoek aan de communicatie (artikel 34 lid 1 concept-wetsvoorstel) wordt gekoppeld aan het verzoek om toestemming voor de verwerving (artikel 33 concept-wetsvoorstel). Dit wordt een combinatielast genoemd.

Er is hier sprake van een continu proces van verwerving en onderzoek aan de verworven communicatie (het gehele linker deel van het schema). Er wordt voortdurend bekeken over welke satellietkanalen en kabels GSM-verkeer van en naar land Y en internetverkeer tussen land Y en land Z wordt getransporteerd en of dit verkeer relevante communicatie voor het onderzoek naar organisatie X bevat. Zo wordt telkens bepaald van welke satellietkanalen en kabels communicatie wordt geïntercepteerd.

In termen van inbreuk op de privacy geldt dat bij de verwerving van de communicatie (fase 1 in het concept-wetsvoorstel) sprake is van een relatief beperkte inbreuk. De inbreuk vindt plaats doordat de communicatie wordt verworven en tijdelijk opgeslagen voor een periode van drie jaar (**paarse blok** in schema). De opgeslagen communicatie betreft ook communicatie die niet relevant is voor het onderzoek van de IVD. De inbreuk is beperkt omdat niet wordt kennisgenomen van de inhoud. Dat is anders bij het onderzoek aan de communicatie (fase 2 in het concept-wetsvoorstel). De inbreuk is hier zwaarder doordat mede aan de hand van de inhoud van de communicatie wordt bepaald over welk satellietkanaal of welke kabel verkeer wordt getransporteerd dat relevant is voor het onderzoek van de IVD.

(Verdere) verwerking (rode blok schema) en voorbewerking (blauwe blok in schema)
Voor het verdere onderzoek naar organisatie X heeft de IVD verschillende mogelijkheden.

Als **eerste mogelijkheid** kan de IVD de bevoegdheid van selectie inzetten (artikel 35 concept-wetsvoorstel). De geschetste casus geeft de mogelijkheid te selecteren aan de hand van de drie telefoonnummers waarvan bekend is dat deze toebehoren aan targets A, B en C. Dit houdt in dat, voor zover gesprekken van en naar de telefoonnummers voorkomen in de verworven communicatie (**paarse blok** in schema), de gesprekken worden geselecteerd en door de IVD mag worden kennisgenomen van deze gesprekken (**rechter paarse lijn** in schema). De casus geeft ook de mogelijkheid te selecteren aan de hand van trefwoorden, bijvoorbeeld 'organisatie X' of de bijnaam van het trainingskamp 'traika'. Dit houdt in dat communicatie waarin deze trefwoorden voorkomen wordt geselecteerd (**rechter paarse lijn** in schema) en de IVD van deze communicatie kennis mag nemen.

Voor de inzet van de bevoegdheid van selectie in het kader van het onderzoek naar organisatie X moet gemotiveerd toestemming worden gevraagd aan de minister (artikel 35 concept-wetsvoorstel). De toestemming wordt verkregen voor drie maanden. De concrete selectiecriteria (telefoonnummers, trefwoorden) hoeven niet aan de minister te worden voorgelegd maar mogen intern de IVD worden vastgesteld.

Wanneer blijkt dat weinig of geen gesprekken van en naar de telefoonnummers van A, B en C voorkomen in de verworven communicatie kan de IVD ervoor kiezen onderzoek te verrichten aan de verworven communicatie (artikel 34 lid 2 concept-wetsvoorstel). Het gaat hier om de bevoegdheid van search gericht op selectie. Het onderzoek aan de communicatie richt zich hier niet op de vraag over welke satellietkanalen en kabels relevante communicatie wordt getransporteerd (search gericht op interceptie), maar op de vraag of met concrete selectiecriteria communicatie kan worden geselecteerd die relevant is voor het onderzoek (search gericht op selectie). De IVD kan bijvoorbeeld onderzoeken of er andere telefoonnummers van A, B en C voorkomen in de verworven communicatie (**rode stippellijn** in schema). Hiervoor moet toestemming worden verkregen van de minister. De toestemming wordt verkregen voor een jaar.

Wanneer door search gericht op selectie telefoonnummers worden verkregen die toebehoren aan A, B, en C kan aan de hand van deze telefoonnummers de communicatie worden geselecteerd (**blauwe lijn** in schema). Hiervoor moet gemotiveerd toestemming worden gevraagd aan de minister. De toestemming wordt verkregen voor drie maanden.

Een **tweede mogelijkheid** voor het verdere onderzoek naar organisatie X is het verrichten van metadata-analyse (artikel 35 concept-wetsvoorstel). In het schema betreft dit de **rechter paarse lijn**. Aanknopingspunten hiervoor zijn de drie bij de dienst bekende telefoonnummers van A, B en C. De metadata-analyse levert bijvoorbeeld een beeld op van telefoonnummers waarmee A, B en C in contact staan. Voor de metadata-analyse gericht op de identificatie van personen, moet gemotiveerd toestemming worden gevraagd aan de minister. De toestemming wordt verkregen voor een jaar.

De IVD kan ervoor kiezen de telefoonnummers waarmee A,B en C in contact staan in selectie te zetten. Hier zal zich doorgaans een motiveringsprobleem voordoen. Uit de metadata-analyse blijkt niet aan wie de telefoonnummers toebehoren. Evenmin is bekend of de contacten relevant zijn voor het onderzoek naar organisatie X. De IVD heeft de mogelijkheid onderzoek aan de communicatie te verrichten (**rode stippellijn** in schema). Personen die in aanmerking komen voor onderzoek door de dienst mogen door middel van search gericht op selectie worden geïdentificeerd (artikel 34, lid 2, onder b concept-wetsvoorstel). Hiervoor moet gemotiveerd toestemming worden gevraagd aan de minister. De toestemming wordt verkregen voor een jaar.

Een **derde mogelijkheid** voor het verdere onderzoek naar organisatie X is het verrichten van onderzoek aan de verworven communicatie (artikel 34 lid 2 concept-wetsvoorstel) aan de hand van andere aanknopingspunten. Een voorbeeld uit de casus zou zijn het zoeken naar telefoonnummers of e-mailadressen van andere leden van organisatie X of van de hoge overheidsfunctionarissen van land Z, zodat ook die communicatie kan worden geselecteerd. Het gaat hier opnieuw om search gericht op selectie (**linker paarse lijn** in schema). Personen die in aanmerking komen voor onderzoek door de dienst mogen door middel van search gericht op selectie worden geïdentificeerd (artikel 34, lid 2, onder b concept-wetsvoorstel). Hiervoor moet gemotiveerd toestemming worden gevraagd aan de minister. De toestemming wordt verkregen voor een jaar. Indien dit onderzoek aan de communicatie gegevens oplevert die relevant zijn voor het onderzoek naar organisatie X (bijvoorbeeld telefoonnummers of e-mailadressen), dan kan vervolgens de selectiebevoegdheid worden ingezet aan de hand van die gegevens (**blauwe lijn** in schema).

Bij de gegeven drie fictieve mogelijkheden voor onderzoek door de IVD is eveneens sprake van continue processen van onderzoek aan de verworven communicatie (d.w.z. search gericht op selectie, metadata-analyse en selectie). Het gaat hier om het onderste deel van het schema. Er wordt voortdurend gezocht naar mogelijkheden om die communicatie die relevant is voor het onderzoek naar organisatie X te selecteren.

De drie fasen corresponderen met de mate van inbreuk op de persoonlijke levenssfeer die aan de orde kan zijn. In termen van inbreuk op de privacy geldt dat bij de selectie van de communicatie (fase 3 in het concept-wetsvoorstel) sprake is van een potentieel vergaande inbreuk. Voor zover communicatie gerelateerd aan de eerder genoemde drie telefoonnummers van targets A, B en C voorkomt in de bulk, wordt deze geselecteerd. Dat houdt in dat deze gegevens voor zolang zij relevant zijn, worden opgeslagen. Van de inhoud wordt kennisgenomen en de communicatie kan worden gebruikt in het inlichtingenproces. Dat is anders bij het onderzoek aan de communicatie (fase 2 in het concept-wetsvoorstel). De inbreuk is hier beperkter. Weliswaar wordt kennisgenomen van de inhoud van de communicatie maar van opslag voor onbepaalde tijd en van het gebruiken van de communicatie is nog geen sprake. Ook bij metadata-analyse (fase 3 in het concept-wetsvoorstel) is sprake van een potentieel vergaande inbreuk. Hier wordt weliswaar geen kennisgenomen van de inhoud van de communicatie, de metadata-analyse kan echter vergaand zicht bieden op bepaalde aspecten van iemands privéleven.

(Verdere) verwerking (**rode blok** in schema) en verwerving (**groene blok** in schema)
De resultaten van metadata-analyse en selectie (of het uitblijven van goede resultaten) kunnen tot bijstelling van de interceptie leiden (**zwarte stippellijn** in schema). Voorbeelden hiervan zijn aanpassing van de keuze van een satellietkanaal, de focus op een ander soort verkeer of het intercepteren van een ander deel van de kabel. Het gaat hier om het rechter deel van het schema.

In het volgende deel beoordeelt de CTIVD aan de hand van de verschillende waarborgen in het concept-wetsvoorstel of het voorgestelde interceptiestelsel duidelijke aanknopingspunten biedt voor toezicht. Deze waarborgen zijn: voorzienbaarheid van de bepalingen, functiescheiding, toestemmingsregime en toestemmingstermijnen.

2.3.2 Voorzienbaarheid van de bepalingen

De waarborg van voorzienbaarheid
De voorzienbaarheid is een belangrijke waarborg tegen ongeoorloofde inbreuken op de persoonlijke levenssfeer. De wet moet voldoende duidelijk en nauwkeurig zijn. Het moet inzichtelijk zijn in welke gevallen de diensten een bevoegdheid mogen uitoefenen en wat hierbij de randvoorwaarden zijn.

Voor het EHRM weegt de eis van voorzienbaarheid extra zwaar in het geval van heimelijk onderzoek. Dit in verband met het risico van misbruik van bevoegdheden. De omstandigheid dat technologie steeds geavanceerder wordt draagt hier volgens het EHRM aan bij.

Samenhang tussen de search- en selectiebevoegdheid

De CTIVD heeft in verschillende toezichtsrapporten problemen geconstateerd in het proces van de verwerving en verwerking van satellietcommunicatie. Deze problemen zagen onder meer op het ontbreken van een wettelijke basis voor bepaalde vormen van search en het ontbreken van een regeling voor metadata-analyse. In beide gevallen kan sprake zijn van een inbreuk op de persoonlijke levenssfeer. In het concept-wetsvoorstel zijn deze bevoegdheden opgenomen in artikel 34 resp. artikel 35. Er is daarmee een wettelijke basis voor deze vormen van search en een regeling voor meta-wdata-analyse gecreëerd. De inhoudelijke waarde hiervan komt later aan de orde.

De CTIVD heeft daarnaast in haar toezichtsrapporten bij herhaling geconstateerd dat de selectiebevoegdheid in de praktijk minder specifiek of gericht is dan waar de huidige wet van uitgaat. Dit komt onder meer tot uiting in het gebruik van (te) generiek geformuleerde verzoeken om toestemming aan de minister. Hierbij worden zogeheten generieke identiteiten gebruikt. Daaronder vallen bepaald 'soorten' personen of organisaties. Wanneer een persoon of organisatie in beeld komt die onder een generieke identiteit valt, kunnen selectiecriteria met betrekking tot die persoon of organisatie direct in selectie worden gezet zonder dat nadere toestemming wordt verkregen. De toestemming voor de generieke identiteit is immers al verkregen. Deze werkwijze is niet in overeenstemming met de Wiv 2002. Naar het oordeel van de CTIVD lopen de huidige wettelijke regeling en de noodzakelijke praktijk op dit punt echter uiteen.[36] Daarnaast is sprake van een grote mate van 'uitproberen': selectie wordt breed ingezet aan de hand van criteria (persoonsgegevens) waarvan de relevantie niet altijd vaststaat. Als gevolg van deze praktijk, wordt selectie in veel gevallen onvoldoende (concreet) gemotiveerd door de diensten. Dit is een al jarenlang aanwezig en door de CTIVD geconstateerd (structureel) probleem.

De bevoegdheid tot selectie is in het concept-wetsvoorstel opgenomen in artikel 35 (**rode blok** in schema). Het verschil met de huidige regeling is dat de selectiecriteria (technische kenmerken als een telefoonnummer of e-mailadres) aan de hand waarvan selectie plaatsvindt niet langer gemotiveerd aan de minister moeten worden voorgelegd. Deze selectiecriteria betreffen persoonsgegevens. De toestemming van de minister voor de inzet van selectie moet worden verkregen aan de hand van, voor zover van toepassing, een omschrijving van het onderwerp, de identiteit van de persoon of organisatie. In de memorie van toelichting wordt uitgelegd dat hier de systematiek van de huidige trefwoordenselectie wordt toegepast: voor het onderwerp (bijvoorbeeld het onderzoek naar organisatie X) wordt toestemming gevraagd, maar voor de concrete selectiecriteria (nummers die toebehoren aan targets A, B en C) niet. Deze selectiecriteria kunnen in mandaat worden vastgesteld, maar moeten (intern) wel worden voorzien van een toereikende motivering in relatie tot het onderzoek, volgens het concept-wetsvoorstel. Het vaststellen van selectiecriteria wordt gezien als een uitvoeringshandeling.[37]

---

[36] Zie nader over het gebruik van generieke identiteiten Toezichtsrapport van de CTIVD nr. 28 inzake de inzet van Sigint door de MIVD, Kamerstukken II 2011/12, 29 924, nr. 74 (bijlage), paragraaf 8.3.3, beschikbaar op www.ctivd.nl.

[37] Memorie van toelichting, p. 97-98.

Deze wijze waarop volgens het concept-wetsvoorstel toestemming dient te worden verkregen voor selectie (artikel 35 van het concept-wetsvoorstel) en de wijze waarop de toestemming dient te worden gemotiveerd biedt op zichzelf nauwelijks een oplossing voor de geconstateerde problemen. Het lijkt de diensten een juridische basis te geven voor het hanteren van generiek geformuleerde (dat wil zeggen weinig specifieke of begrensde) aanvragen aan de minister. (In de fictieve casus zou het bijvoorbeeld gaan om een verzoek om toestemming voor de inzet van de selectiebevoegdheid ten aanzien van de communicatie van personen gerelateerd aan organisatie X). Een ministeriële toestemming is noodzakelijk voor het inzetten van de selectiebevoegdheid in een onderzoek maar niet voor de selectiecriteria die gerelateerd zijn aan dit onderzoek. Er wordt meer flexibiliteit bewerkstelligd bij het toevoegen van selectiecriteria aangezien de gang naar de minister hiervoor niet noodzakelijk is.

Aan het eerder door de CTIVD geconstateerde motiveringsprobleem verandert het concept-wetsvoorstel echter weinig. Volgens het concept-wetsvoorstel moet ieder selectiecriterium intern immers nog steeds worden voorzien van een toereikende motivering. Het verschil is enkel gelegen in het niveau waarop toestemming dient te worden verkregen. In het verleden heeft de CTIVD geconstateerd dat een deugdelijke motivering bij veel selectiecriteria (te gebruiken persoonsgegevens) ontbrak en dat deze in veel gevallen ook niet mogelijk is. (Bijvoorbeeld wanneer telefoonnummers in selectie worden gezet waarvan op dat moment nog niet duidelijk is of en op welke wijze deze relevant zijn voor het onderzoek. In de fictieve casus zou het kunnen gaan om de kring van personen met wie targets A, B en C in contact staan). Dit probleem zal zich ook voordoen indien de selectiecriteria intern worden vastgesteld. Ook dan is een toereikende motivering immers terecht vereist. Volgens de CTIVD moet de oplossing voor dit probleem overigens niet gezocht worden in het loslaten van deze motiveringseis.

Het concept-wetsvoorstel biedt in artikel 34 (**blauwe blok** in schema) de diensten de mogelijkheid de relevantie van selectiecriteria door middel van de searchbevoegdheid te onderzoeken (lid 2 van artikel 34, **rode stippellijn** in schema). Door middel van deze bevoegdheden kunnen de diensten vooraf uitzoeken of selectiecriteria waarvan de relevantie nog niet vaststaat inderdaad relevant zijn, onder meer door personen te identificeren die in aanmerking komen voor onderzoek. Selectiecriteria die op basis hiervan niet relevant worden beoordeeld, dienen volgens de CTIVD niet in selectie te worden geplaatst. Selectiecriteria die wel relevant zijn, kunnen vervolgens afdoende gemotiveerd worden bij het in selectie plaatsen. Een dergelijk onderzoek op basis van artikel 34 kan als noodzakelijk "vooronderzoek" dienen voor toepassing van de selectiebevoegdheid. Het ten onrechte achterwege laten van deze stap zal volgens de CTIVD van invloed zijn op de rechtmatigheid van de selectie. De CTIVD wijst erop dat een minder grote inbreuk wordt gemaakt op de persoonlijke levenssfeer bij toepassing van de searchbevoegdheid dan bij de selectiebevoegdheid. In beide gevallen wordt weliswaar kennisgenomen van de inhoud van communicatie, maar het toegestane doel bij de searchbevoegdheid is beperkt tot de identificatie van bekende en nieuwe onderzoekssubjecten. Dit leidt ertoe dat een beperkte inbreuk op de persoonlijke levenssfeer mag worden gemaakt zodat een verdergaande inbreuk zoveel als mogelijk wordt voorkomen.

De CTIVD merkt op dat het voorgestelde artikel 34 op onderdelen hieronder wordt besproken. Zij ziet op verschillende punten aanleiding het voorgestelde artikel 34 aan te passen dan wel te verduidelijken, onder meer op het punt van de voorzienbaarheid van de bepaling. In de huidige vorm biedt artikel 34 naar het oordeel van de CTIVD onvoldoende waarborgen om betiteld te kunnen worden als minder inbreukmakend vooronderzoek.

Advies

De CTIVD adviseert de bevoegdheid van search gericht op selectie, mits voldoende afgebakend, toe te passen als een voorportaal van selectie en dit expliciet op te nemen in de memorie van toelichting.

Onderscheid technisch en inhoudelijk onderzoek aan gegevens

Het concept-wetsvoorstel en de memorie van toelichting maken onvoldoende duidelijk wat het onderscheid is tussen de verschillende vormen van technisch en inhoudelijk onderzoek aan gegevens. Zo lijkt sprake te zijn van een overlap tussen technische analyse (artikel 33, lid 1; **groene blok** in schema) en search gericht op interceptie (artikel 34, lid 1, onder a; **linker paarse lijn** in schema). Beide bevoegdheden geven ruimte voor de technische verkenning van gegevens, bijvoorbeeld het vaststellen van de aard van het verkeer of de geografische afbakening daarvan, eventueel door het inhoudelijk kennisnemen van de verworven communicatie. Het wordt niet duidelijk waarin deze bevoegdheden van elkaar verschillen. Het mogen verrichten van technische analyse onder artikel 33 ligt besloten in de toestemming voor interceptie. Voor technische analyse onder artikel 33 hoeft geen separate toestemming te worden verkregen van de minister. Dit volgt in ieder geval niet uit het concept-wetsvoorstel of de memorie van toelichting. In het geval van search gericht op interceptie (artikel 34, lid 1) dient hier wel expliciet toestemming voor te worden verkregen. Hierin ligt een extra waarborg besloten die bij artikel 33 ontbreekt.

Advies

De CTIVD adviseert duidelijkheid te bieden over het onderscheid tussen technische analyse (artikel 33) en search gericht op interceptie (artikel 34).

Onderscheid tussen verschillende searchvormen

Een overlap lijkt zich ook voor te doen bij search gericht op interceptie (artikel 34, lid 1) en search gericht op selectie (artikel 34, lid 2). Beide bevoegdheden geven ruimte voor inhoudelijk onderzoek gericht op het identificeren of de identificatie van personen of organisaties die in aanmerking komen voor (toekomstig) onderzoek. Wat is het onderscheid tussen deze bevoegdheden? In de memorie van toelichting worden weliswaar voorbeelden genoemd, maar de verschillende vormen worden niet in onderlinge verhouding met elkaar verduidelijkt.

Advies

De CTIVD adviseert het onderscheid tussen de verschillende searchvormen nader te verduidelijken.

Nadere kennisneming

Volgens de CTIVD geeft de term ‘nadere kennisneming’ in het zesde lid van het voorgestelde artikel 34 (**blauwe lijn** in schema) een onjuiste beeld van de activiteit. Bij het onderzoek aan gegevens (search) wordt immers al kennisgenomen van de inhoud van de communicatie. Het kan onder omstandigheden zo zijn dat de communicatie waarvan wordt kennisgenomen van direct en onmiddellijk belang is voor het inlichtingenproces (bijvoorbeeld bij een aanslagdreiging). Een verzoek om toestemming voor gerichte interceptie (voorgesteld artikel 32) of selectie (voorgesteld artikel 35) moet dan worden ingediend. Het gaat dan niet om ‘nadere kennisneming’, maar om kennisneming door anderen of om het gebruiken van deze communicatie. De kennisneming bij search is (in tegenstelling tot de huidige bevoegdheid) immers niet beperkt in tijd (kortstondig) of in functie (voor zover noodzakelijk om …).

Advies

De CTIVD adviseert in het concept-wetsvoorstel een passender benaming voor de activiteit in artikel 34 te kiezen.

Selectie

De zinsnede 'voor zover van toepassing, de identiteit van de persoon of organisatie of een omschrijving van het onderwerp' in voorgesteld artikel 35 lid 2 (**rode blok** en **rechter paarse lijn** in schema) laat ruimte voor interpretatie en wordt niet nader toegelicht. Het is daardoor onvoldoende duidelijk wat precies wordt bedoeld.

In de memorie van toelichting wordt aangegeven dat geen onderscheid meer wordt gemaakt in de drie categorieën van selectiecriteria (gegevens betreffende de identiteit, nummer, trefwoord), maar dat voor één toestemmingsregime is gekozen. Ook wordt opgemerkt dat het van belang is dat een voldoende afgebakende omschrijving wordt gegeven van het onderzoek waarvoor de toestemming tot selectie wordt gevraagd. Dat moet zo specifiek en nauwkeurig mogelijk worden omschreven. Ter uitvoering van de verleende toestemming kunnen vervolgens in mandaat selectiecriteria worden vastgesteld. Toestemming is niet vereist van de minister maar van het hoofd van de dienst. Deze selectiecriteria moeten intern wel toereikend worden gemotiveerd.[38]

Het is de CTIVD niet duidelijk of met het voorgestelde artikel 35 lid 2 is bedoeld ruimte te laten voor een omschrijving waaruit slechts hoeft te blijken om wat voor 'soort' persoon of organisatie het gaat. In de fictieve casus zou het bijvoorbeeld gaan om personen gerelateerd aan organisatie X. Een ander voorbeeld is de piraat als 'soort' persoon. Dit zou het gebruik toestaan van een zogeheten generieke identiteit. Onder een generieke identiteit valt een bepaald soort personen of organisaties. In de huidige wet is het opnemen van concrete gegevens betreffende de identiteit van een persoon of organisatie vereist. In de fictieve casus zou het bijvoorbeeld gaan om persoon D, die in contact staat met targets A en B. In het andere voorbeeld zou het gaan om de concrete persoon die als piraat kan worden aangemerkt. De CTIVD heeft in een eerder toezichtsrapport aangegeven onder bepaalde omstandigheden niet negatief te staan tegenover het gebruik van generieke identiteiten. Deze omstandigheden zien onder meer op de situatie dat in een zeer korte periode een informatiepositie moet worden opgebouwd, bijvoorbeeld in het geval van een kaping van een Nederlands schip door piraten. De CTIVD concludeerde echter dat de Wiv 2002 hiervoor niet de ruimte biedt. Naar het oordeel van de CTIVD lopen de huidige wettelijke regeling en de noodzakelijke praktijk op dit punt uiteen.[39]

Advies

De CTIVD adviseert nader toe te lichten of het concept-wetsvoorstel het gebruik van generieke identiteiten thans beoogt te regelen. Indien dit het geval is, adviseert zij duidelijker te maken welke kaders hiervoor dienen te gelden.

Het is de CTIVD niet duidelijk hoe het toestemmingsregime wordt toegepast in het geval geen identiteit bekend is. Een voorbeeld hiervan is dat het nummer naar voren komt in het onderzoek naar organisatie X of naar piraterij, maar het is niet bekend aan wie het nummer toebehoort. Volstaat dan de verleende toestemming voor de inzet van selectie aan de hand van de omschrijving van het onderzoek? Met andere woorden, moet 'voor zover van toepassing' in artikel 35 gelezen worden als 'voor zover bekend'? Of ligt hier inzet van een searchbevoegdheid voor de hand, als 'vooronderzoek' voor de inzet van de selectiebevoegdheid? De memorie van toelichting bij het voorgestelde artikel geeft nu geen antwoord op deze vragen. Naar het oordeel van de CTIVD moet het concept-wetsvoorstel, met het oog op de voorzienbaarheid, zo min mogelijk interpretatieruimte laten waar het gaat om het toestemmingsvereiste voor de inzet van een bijzondere bevoegdheid.

---

[38] Zie hierover nader het onderdeel "samenhang tussen search- en selectiebevoegdheid" beschreven in hoofdstuk 2.3.2 van deze reactie.

[39] Zie nader over het gebruik van generieke identiteiten toezichtsrapport van de CTIVD nr. 28 inzake de inzet van Sigint door de MIVD, *Kamerstukken II* 2011/12, 29 924, nr. 74 (bijlage), paragraaf 8.3.3, beschikbaar op www.ctivd.nl.

Advies
De CTIVD adviseert nader toe te lichten hoe de zinsnede "voor zover van toepassing" in artikel 35 dient te worden gelezen.

Metadata-analyse
De bepaling over het verrichten van metadata-analyse (voorgesteld artikel 35; **rode blok** en **rechter paarse lijn** in schema) is volgens de CTIVD te beperkt geformuleerd. Wanneer de metadata-analyse is gericht op het identificeren van personen of organisaties, moet daarvoor toestemming worden verkregen van de minister volgens het concept-wetsvoorstel. De term 'identificeren van personen of organisaties' dekt de lading echter niet. Een inbreuk op de persoonlijke levenssfeer kan namelijk ook plaatsvinden door metadata-analyse gericht op bepaalde patronen, zonder dat het gaat om het identificeren van een persoon of organisatie. Hier kan bijvoorbeeld gedacht worden aan het in kaart brengen van locaties waar iemand zich heeft bevonden of websites die iemand heeft bezocht. Dit wordt in de memorie van toelichting weliswaar aangegeven, maar komt niet tot zijn recht in het voorgestelde wetsartikel.

Advies
De CTIVD adviseert expliciet in het concept-wetsvoorstel tot uiting te laten komen dat ook andere vormen van metadata-analyse die een inbreuk maken op de persoonlijke levenssfeer onder het bereik van het voorgestelde artikel 35 lid 2 kunnen vallen.

Het tweede lid van artikel 47 maakt een niet-limitatieve opsomming van de vormen van geautomatiseerde data-analyse op de inhoud van gegevensbestanden die kunnen worden verricht door de diensten. Het concept-wetsvoorstel schept daarmee de mogelijkheid dat ook andere, nieuwe vormen van geautomatiseerde data-analyse zijn toegestaan. Het voorgestelde artikel 35 over metadata-analyse verwijst echter enkel naar de nu genoemde vormen van geautomatiseerde data-analyse van gegevensbestanden in het voorgestelde artikel 47. Hieruit kan de conclusie volgen dat nieuwe vormen van geautomatiseerde data-analyse niet vallen onder het bereik van het voorgestelde artikel 35 lid 4. Voor nieuwe vormen van geautomatiseerde data-analyse zou dan geen ministeriële toestemming zijn vereist.

Advies
De CTIVD adviseert in de memorie van toelichting expliciet te maken dat ook nieuwe vormen van geautomatiseerde data-analyse onder het bereik kunnen vallen van artikel 35 lid 2 voor zover een inbreuk wordt gemaakt op de persoonlijke levenssfeer.

2.3.3 Functiescheiding

[artikelen 32 lid 4, 33 lid 4, 34 lid 5; p. 59, 68, 73 MvT]

Concept-wetsvoorstel
Het concept-wetsvoorstel introduceert in verschillende artikelen het vereiste van functiescheiding. Dit houdt in dat de minister, of gemandateerd het hoofd van de dienst, aan hem ondergeschikte ambtenaren kan aanwijzen, en aan hen toestemming kan verlenen bij uitsluiting van anderen kennis te nemen van verzamelde gegevens.

De waarborg van functiescheiding

De functiescheiding heeft tot doel te waarborgen dat communicatie waarvan wordt kennisgenomen, niet kan worden gebruikt in het inlichtingenproces zonder dat daaraan een inhoudelijke afweging en toestemming op het juiste niveau vooraf is gegaan.

Systeemtechnische scheiding

Het concept-wetsvoorstel noch de memorie van toelichting gaat in op een systeemtechnische scheiding. Volgens de CTIVD is een systeemtechnische scheiding een noodzakelijke ondersteuning van de functiescheiding. Een systeemtechnische scheiding betekent dat gegevens die op basis van artikel 33 zijn geïntercepteerd op een apart (computer)systeem worden opgeslagen. Deze gegevens zijn dan ook fysiek enkel toegankelijk voor personen die op basis van het wetsvoorstel rechtstreeks daarvan kennis mogen nemen (artikel 33, lid 4 en artikel 34, lid 5). Dit (computer)systeem mag niet rechtstreeks toegankelijk zijn voor personen die betrokken zijn bij het verdere inlichtingenproces (de teams die operationeel onderzoek verrichten).

Advies

De CTIVD adviseert in de memorie van toelichting bij het concept-wetsvoorstel te beschrijven dat een systeemtechnische scheiding onderdeel zal uitmaken van de wettelijke functiescheiding.

Functiescheiding bij artikel 33

Naar het oordeel dient de eis van functiescheiding te vervallen bij artikel 33 (**groene blok** in schema) voor zover deze betrekking heeft op andere activiteiten dan het ongedaan maken van de versleuteling. Er dient een strikt onderscheid te worden gemaakt tussen technische analyse op basis van artikel 33 en search gericht op interceptie (artikel 34, **blauwe blok** in schema). De CTIVD is van oordeel dat onder artikel 33 de technische analyse niet met zich zou mogen brengen dat kennis wordt genomen van de inhoud van communicatie. De eis van functiescheiding is in dat geval dan ook overbodig. Voor zover het in deze gevallen noodzakelijk is kennis te nemen van de inhoud, dient toestemming te worden verkregen voor de toepassing van search gericht op interceptie (artikel 34).

Advies

De CTIVD adviseert de eis van functiescheiding te laten vervallen voor zover deze betrekking heeft op andere activiteiten dan het ongedaan maken van de versleuteling.

Functiescheiding bij search

Aan het vastleggen van de resultaten van onderzoek aan gegevens (search, artikel 34 lid 3, **blauwe blok** in schema) moeten, in het verlengde van de functiescheiding, duidelijke beperkingen worden gebracht. De waarborg van de functiescheiding is essentieel bij de uitvoering van de searchbevoegdheid. Dit dient ook zijn weerslag te krijgen in de wettelijke bepaling over het vastleggen van de searchresultaten. In voorgesteld artikel 34 lid 3 is opgenomen dat van de resultaten van search aantekening mag worden gemaakt indien dat noodzakelijk is voor de goede taakuitvoering. In de memorie van toelichting wordt aangegeven dat deze resultaten verder gebruikt kunnen worden voor het doel waarvoor deze zijn opgetekend. Dat betekent dat kennisneming van de resultaten door medewerkers van de dienst is beperkt volgens het *need-to-know*-principe. Er worden geen verdere beperkingen aangebracht op het vastleggen van de resultaten. Het is onvoldoende duidelijk welke gegevens wel en niet mogen worden vastgelegd. Noodzakelijkheid voor de taakuitvoering is daarin een te algemeen begrip en geeft te veel ruimte. Het gevaar bestaat dat de waarborg van functiescheiding in de praktijk wordt uitgehold door uitgebreide vastlegging van de resultaten van search.

Advies
De CTIVD adviseert in het concept-wetsvoorstel adequate waarborgen in te bouwen voor het vastleggen en (nader) verwerken van de searchresultaten.

Functiescheiding bij metadata-analyse en vaststelling selectiecriteria
Het concept-wetsvoorstel voorziet onnodig in functiescheiding bij de uitoefening van metadata-analyse en bij het vaststellen van selectiecriteria (voorgesteld artikel 35 lid 5, **rode blok** in schema). De functiescheiding impliceert dat sprake is van kennisneming van inhoudelijke communicatie die niet zonder meer gebruikt mag worden in het inlichtingenproces. Daar is bij het vaststellen van selectiecriteria slechts sprake van indien gebruik wordt gemaakt van de mogelijkheid van search. Voorgesteld artikel 34 lid 3 voorziet dan in de waarborg van functiescheiding; een tweede bepaling is niet nodig. Ook bij metadata-analyse is geen sprake van inhoudelijke kennisname, althans dat blijkt niet uit het concept-wetsvoorstel. Voor het nader duiden op relevantie voor het onderzoek van de uitkomsten van metadata-analyse (bijvoorbeeld de personen met wie targets A, B en C in contact staan) aan de hand van de inhoud van de communicatie geeft artikel 35 geen mogelijkheid. Een functiescheiding als waarborg tegen ongeoorloofde inbreuken op de persoonlijke levenssfeer heeft hier geen meerwaarde.

Advies
De CTIVD adviseert de eis van functiescheiding te laten vervallen in artikel 35 lid 5.

Functiescheiding bij gebruik scanapparatuur t.b.v. gerichte interceptie
De waarborg van functiescheiding moet worden gesteld in alle gevallen van inhoudelijke kennisneming die ter ondersteuning van een bevoegdheid plaatsvindt. Dit geldt ook voor inhoudelijke kennisneming bij het gebruik van scanapparatuur om ten behoeve van gerichte interceptie een nummer vast te stellen (voorgesteld artikel 32 lid 4). Deze waarborg ontbreekt.

Advies
De CTIVD adviseert de waarborg van functiescheiding in artikel 32 te introduceren.

2.3.4 Toestemmingsregime en gelimiteerde toestemmingstermijnen

[artikelen 33 lid 2, 34 lid 4, 35 lid 2; p. 64, 67-68, 70, 72, 76 MvT]

Verzoek om toestemming voor search
Aan verzoeken om toestemming voor het verrichten van onderzoek aan gegevens (search, artikel 34, **blauwe blok** in schema) moeten volgens de CTIVD aanvullende vereisten worden gesteld. Zo zou in het verzoek moeten worden opgenomen waaruit het onderzoek aan de gegevens precies bestaat en welke concrete vragen het onderzoek beoogt te beantwoorden. Bij onderzoek aan gegevens waarbij sprake is van het vaststellen en verifiëren van selectiecriteria of het identificeren van personen of organisaties die in aanmerking komen voor (toekomstig) onderzoek zou ook moeten worden opgenomen wat de aanleiding is voor het onderzoek aan de gegevens. Het voorgestelde artikel 34 stelt nu geen aanvullende eisen. Dit maakt het verzoek om toestemming onvoldoende concreet en slechts beperkt toetsbaar.

Advies
De CTIVD adviseert in het concept-wetsvoorstel aanvullende eisen te stellen aan het verzoek om toestemming voor artikel 34.

Toestemmingsperiode voor bepaalde vormen van search

De periode waarvoor toestemming wordt verleend moet volgens de CTIVD bij bepaalde vormen van search worden beperkt tot drie maanden. In het wetsvoorstel is een termijn opgenomen van twaalf maanden. Dit betreft het onderzoek aan gegevens gericht op het vaststellen en verifiëren van selectiecriteria en om het identificeren van personen of organisaties die in aanmerking komen voor (toekomstig) onderzoek (artikel 34, lid 2; **rode stippellijn** in schema). De searchbevoegdheid is weliswaar niet gericht op het gebruiken van de inhoud van de communicatie, maar is wel nadrukkelijk gericht op het kennisnemen van de inhoud van de communicatie gerelateerd aan concrete personen en organisaties. Vanwege de inbreuk op de persoonlijke levenssfeer moet de toestemmingsperiode worden beperkt tot drie maanden.

Advies
De CTIVD adviseert in het concept-wetsvoorstel de toestemmingstermijn voor artikel 34 lid 2 te beperken tot drie maanden.

Toestemmingsperiode voor geautomatiseerde data-analyse, waaronder metadata-analyse

De periode waarvoor toestemming wordt verleend bij inbreukmakende vormen van metadata-analyse en geautomatiseerde data-analyse die de inhoud van gegevensbestanden betreft, moet volgens de CTIVD worden beperkt tot drie maanden. Dit betreft die vormen van analyse die zijn gericht op het identificeren van personen en organisaties of het onderkennen van bepaalde patronen, waardoor inbreuk wordt gemaakt op de persoonlijke levenssfeer. Het voorgestelde artikel 35 lid 4 gaat nu uit van een periode van twaalf maanden. Waarom voor een dergelijke lange periode is gekozen, wordt niet nader toegelicht. Vanwege de inbreuk op de persoonlijke levenssfeer, die onder omstandigheden aanzienlijk kan zijn (en vergelijkbaar is met selectie), dient volgens de CTIVD een periode van drie maanden te worden gehanteerd.

Advies
De CTIVD adviseert in het concept-wetsvoorstel de toestemmingstermijn voor artikel 35 lid 5 te beperken tot drie maanden.

Inbreuk op de persoonlijke levenssfeer bij de inzet van selectie

De CTIVD plaatst een kanttekening bij de stelling in de memorie van toelichting dat de inbreuk op de persoonlijke levenssfeer minder groot is bij de toepassing van de selectiebevoegdheid (artikel 35) dan bij het gericht intercepteren van communicatie (bijv. door een telefoontap, artikel 32). In de memorie van toelichting staat dat de inbreuk bij selectie minder vergaand is omdat niet real time en online kennis wordt genomen van communicatie. Bovendien wordt niet kennisgenomen van alle communicatie van de betrokkene maar uitsluitend de communicatie die in bulk is geïntercepteerd. De CTIVD merkt op dat de potentiële inbreuk in ieder geval vergelijkbaar is met de inbreuk bij gerichte interceptie. Zo voorziet het concept-wetsvoorstel in een bewaartermijn van drie jaar waardoor het mogelijk is ver terug te kijken.

Deze mogelijkheid bestaat niet bij gerichte interceptie. Daarnaast kan de communicatie die in bulk is geïntercepteerd van een grote verscheidenheid aan telecommunicatiebronnen afkomstig zijn (bijv. buitenlandse telefoongesprekken, internetverkeer). Dit kan tot meer gegevens leiden dan het geval zou zijn bij het gericht intercepteren van weliswaar alle communicatie maar wel van slechts één telefoonnummer.[40]

2.4 Conclusie

In dit hoofdstuk heeft de CTIVD onderzocht of het concept-wetsvoorstel voldoende houvast biedt voor het uitoefenen van toezicht. Zij komt tot de conclusie dat dit niet altijd het geval is. Het wetsvoorstel schiet op dit punt op verschillende onderdelen tekort. Vooral op het terrein van het verschaffen van duidelijkheid over en nauwkeurige omschrijvingen van de voorgestelde bepalingen ziet de CTIVD ruimte voor verbetering. Dit geldt zowel voor het interceptiestelsel (artikelen 32-35) als voor de regeling voor de inzet van bijzondere bevoegdheden ter ondersteuning van de goede taakuitvoering (artikel 23 lid 2).

Het concept-wetsvoorstel en de memorie van toelichting bieden onvoldoende duidelijkheid over de reikwijdte van de besproken bevoegdheden. Hierdoor zal het voor de CTIVD niet altijd mogelijk zijn effectief toezicht op uit te oefenen. Vereist hiervoor is immers dat helder is binnen welke strikte kaders de AIVD en de MIVD dienen te blijven bij de uitoefening van hun bevoegdheden.

[40] Zie ook *Het mensenrechtenkader voor het Nederlandse stelsel van toezicht op de inlichtingen- en veiligheidsdiensten*, J.P. Loof, J. Uzman, T. Barkhuysen, A.C. Buyse, J.H. Gerards & R.A. Lawson, augustus 2015, p. 17-18, te raadplegen via www.ctivd.nl.

3 Waarborgen voor de bescherming van de privacy

3.1 Inleiding

Het concept-wetsvoorstel geeft de CTIVD aanleiding tot een aantal opmerkingen dat niet in een rechtstreeks verband staat tot het kunnen uitoefenen van effectief toezicht. Het gaat om thema's of specifieke bepalingen waarin naar het oordeel van de CTIVD de privacy-waarborgen ontbreken of onvoldoende zijn. De CTIVD vindt het belangrijk deze opmerkingen te plaatsen omdat het voor de buitenwereld – dat wil zeggen degenen die geen kennis hebben van de werking van een dergelijke wet in de praktijk – niet altijd helder zal zijn dat een waarborg ontbreekt en hoe groot de gevolgen daarvan kunnen zijn. De vraag die in dit hoofdstuk dan ook centraal staat is: **Waar ontbreken nog adequate waarborgen voor de bescherming van de privacy?**

Onderwerpen die aan de orde komen zijn naslag en gegevensverstrekking op verzoek, vernietiging van de gegevens van informanten en agenten, de inzet van bijzondere bevoegdheden jegens journalisten, de hackbevoegdheid, bewaartermijnen voor verzamelde gegevens, geautomatiseerde data-analyse, het bevorderen of treffen van maatregelen door de diensten en de samenwerking met buitenlandse inlichtingen- en veiligheidsdiensten.

De adviezen van de CTIVD zijn telkens in een **kader** weergegeven. Aan het einde van het hoofdstuk volgt een korte algemene conclusie waarin wordt ingezoomd op de hoofdlijnen om een antwoord te geven op de centrale vraag.

3.2 Naslag en gegevensverstrekking op verzoek

[artikelen 8 lid 2 sub f, 10 lid 2 sub g, en 50; p. 10-13 MvT]

Concept-wetsvoorstel

Het concept-wetsvoorstel voorziet in een nieuw taakelement voor de AIVD en de MIVD: het doen van een mededeling omtrent door de dienst verwerkte gegevens met betrekking tot personen of instanties, op verzoek van bij regeling aangewezen personen of instanties, in gevallen die in de regeling zijn aangewezen (artikel 8 lid 2 sub f en artikel 10 lid 2 sub g). Het gaat hier om het doen van een naslag in de bestanden van de dienst en het vervolgens verstrekken van die gegevens aan bepaalde belangendragers. Bij dit nieuwe taakelement hoort ook een bepaling die ziet op de externe verstrekking van de informatie die uit de naslag naar voren komt (artikel 50).

Aandachtspunten

De CTIVD heeft in haar rapport nr. 36 gesignaleerd dat voor de bestaande praktijk van naslagen naar bepaalde categorieën personen door de AIVD geen specifieke wettelijke basis bestaat in de huidige Wiv.[41] Het ging daarbij bijvoorbeeld om verzoeken door partijvoorzitters om kandidaat-Kamerleden na te slaan in de bestanden van de AIVD, als daar een bepaalde aanleiding voor bestaat. Ook vallen de naslagen die standaard plaatsvinden naar kandidaat-bewindspersonen en naar kandidaten voor het ambt van Commissaris van de Koning, burgemeester, (waarnemend) rijksvertegenwoordiger of gezaghebber BES onder deze categorie. Een ander voorbeeld is de naslag naar potentiële leden van de koninklijke familie. Bij alle voornoemde soorten naslagen zag de CTIVD voldoende raakvlakken met de algemene taak van de AIVD in het belang van de nationale veiligheid om de praktijk rechtmatig te achten.

---

[41] Toezichtsrapport van de CTIVD nr. 36 inzake het vervolgonderzoek naar de door de AIVD uitgebrachte ambtsberichten betreffende (kandidaat) politieke ambtsdragers en potentiële leden van de koninklijke familie, *Kamerstukken II*

Zij kon de naslagen echter niet onderbrengen onder een van de specifieke taken van de dienst. Dit is in het kader van de kenbaarheid en voorzienbaarheid van inbreuken op de persoonlijke levenssfeer wel vereist.

Een gemene deler bij de voornoemde voorbeelden van naslagen is dat het gaat om categorieën die bezwaarlijk onder de regeling van vertrouwensfuncties kunnen worden gebracht. De ambten of posities waar het om gaat zijn (met uitzondering van potentiële leden van de koninklijke familie) een direct of indirect uitvloeisel van een democratische verkiezing. Daarom dient de keuze van de persoon die een dergelijke ambt of positie vervult niet afhankelijk te worden gemaakt van een beoordeling door de uitvoerende macht. Het aanwijzen van de positie van potentieel lid van de koninklijke familie als vertrouwensfunctie stuit om voordehand liggende redenen op bezwaren. Vanwege het staatsbelang bij het verminderen van risico's bij de vervulling van deze ambten/posities, is de CTIVD van oordeel dat een naslag in de eigen bestanden van de AIVD gerechtvaardigd is. Vanuit rechtstatelijk perspectief biedt dit het voordeel dat de diensten geen vetorecht krijgen zoals dat wel het geval is als een Verklaring van Geen Bezwaar (VGB) wordt geweigerd in het kader van een vertrouwensfunctie. De informatie die de diensten verstrekken kan door de belanghebbende partij (bijvoorbeeld de partijvoorzitter) worden meegewogen in de beslissing over het al dan niet aanstellen van de persoon.

Tegen deze achtergrond ziet de CTIVD het voorbeeld dat gegeven wordt in de memorie van toelichting, te weten een naslag ten behoeve van vitale bedrijven bij essentiële functies, als een vreemde eend in de bijt. In dergelijke situaties is er geen reden af te wijken van de hoofdregel: de regeling van vertrouwensfuncties. Indien een functie als 'essentieel' kan worden aangemerkt in relatie tot de nationale veiligheid, dan ligt het voor de hand deze functie aan te wijzen als vertrouwensfunctie. De CTIVD wijst erop dat het aanwijzen van een functie als vertrouwensfunctie de voorkeur verdient, omdat dan kenbaar is voor personen die de functie ambiëren dat zij een veiligheidsonderzoek zullen moeten ondergaan. Een andere reden te kiezen voor de vertrouwensfunctie-regeling is dat deze geldt voor alle personen die voor een bepaalde functie in aanmerking komen. Indien een functie vanuit veiligheidsperspectief gevoelig is, vormt dit een reden in alle gevallen zicht te krijgen op de mogelijke risico's die met de functionaris samenhangen. Het gaat daarbij dus ook om de risico's waar de werkgever op voorhand geen indicatie van zal hebben.

De CTIVD merkt tevens op dat de herkomst van een persoon als mogelijke aanleiding voor het verzoek om een naslag wordt genoemd in de memorie van toelichting. Zij acht dit onjuist met het oog op artikel 1 van de Grondwet en artikel 14 van het EVRM. De herkomst van een persoon vormt op zichzelf geen valide aanleiding voor een naslagverzoek. Wel kan dit, in combinatie met andere factoren (b.v. een recent verblijf in een bepaald gebied), voldoende reden zijn.

Advies

De CTIVD adviseert de memorie van toelichting te wijzigen met betrekking tot het scheppen van de mogelijkheid de naslagregeling toe te passen ten aanzien van vitale bedrijven. Voor vitale bedrijven zou uitsluitend de regeling van vertrouwensfuncties moeten gelden.

Voorts adviseert de CTIVD de ministers het voorbeeld dat de herkomst van een persoon een gerechtvaardigde aanleiding kan vormen voor een naslagverzoek te verwijderen uit de memorie van toelichting.

2012/13, 29 924, nr. 104 (bijlage), beschikbaar op www.ctivd.nl, para. 3.1 en 4.1.

3.3 Vernietiging van de gegevens van informanten en agenten

[artikelen 22 lid 5 en 26 lid 8; p. 27-28 MvT]

Concept-wetsvoorstel

In het wetsontwerp wordt voorgesteld informanten- en agentendossiers van de AIVD en de MIVD te vernietigen na een periode van 30 jaar. De voorgestelde bepaling is analoog aan artikel 12 van de Wet politiegegevens. De argumenten genoemd in de memorie van toelichting zijn de veiligheidsrisico's en de toezegging van absolute geheimhouding.

Aandachtspunten

Er heeft in het verleden langdurig overleg plaatsgevonden – ook met de Tweede Kamer – over het overbrengen van de archieven van de AIVD en de MIVD naar het Nationaal Archief. Het overbrengen gebeurt op basis van een selectielijst. Volgens de Archiefwet moet in een selectielijst worden aangegeven welke gegevens moeten worden vernietigd en welke gegevens voor overbrenging naar het Nationaal Archief in aanmerking komen. De lijst wordt vastgesteld door de ministers van BZK (voor de AIVD) of Defensie (voor de MIVD) en de minister van Onderwijs, Cultuur en Wetenschap. De overdracht van informanten- en agentendossiers is een struikelblok gebleken voor de vaststelling van een selectielijst voor de AIVD en de MIVD.[42] De commissie Dessens heeft geoordeeld dat de Archiefwet voldoende mogelijkheden biedt om de geheimhouding van deze dossiers voor zeer lange tijd (een periode van meer dan 100 jaar) te waarborgen.[43]

De CTIVD wijst erop dat met de keuze in het concept-wetsvoorstel voor een vernietigingstermijn van 30 jaar, de beantwoording van informatieverzoeken van familie en/of nabestaanden substantieel wordt beperkt.

De stelling dat te beschermen gegevens van menselijke bronnen zodanig verweven zijn met de archiefbestanden dat ook het archief daaromheen niet overgedragen kan worden, gaat te ver. Het draagt ook niet bij aan het in een democratie essentiële vereiste van verantwoording en rekenschap achteraf. Het is juist een teken van kracht deze gegevens zodanig toegankelijk te maken voor wetenschappelijk onderzoek en naslag dat ook onderzoek naar dit aspect van het eigen functioneren van de AIVD en de MIVD mogelijk wordt gemaakt. Daarbij neemt de CTIVD in aanmerking dat de AIVD en de MIVD de reikwijdte van het begrip gegevens over agenten en informanten ruim definiëren, in elk geval ruimer dan enkel hun identiteitsgegevens.

Advies

De CTIVD adviseert de voorgestelde bepalingen in het bredere kader van historisch perspectief te beoordelen en een oplossing te zoeken in de mogelijkheden die de Archiefwet biedt.

---

[42] Zie hierover paragraaf 10.1 van het toezichtsrapport van de CTIVD nr. 33 inzake de rubricering van staatsgeheimen door de AIVD, *Kamerstukken II* 2011/12, 30 977, nr. 47 (bijlage), beschikbaar op www.ctivd.nl.

[43] Naar een nieuwe balans tussen waarborgen en bevoegdheden, evaluatie Wet op de inlichtingen- en veiligheidsdiensten, commissie Dessens, december 2013, *Kamerstukken II* 2013/14, 33 820, nr. 1, p. 162.

3.4 Inzet van bijzondere bevoegdheden jegens journalisten

[artikel 24 vierde lid; p. 35 MvT]

Concept-wetsvoorstel

Het vierde lid van artikel 24 regelt de uitoefening van bijzondere bevoegdheden jegens een journalist voor zover de uitoefening is gericht op het achterhalen van de bron van een journalist.[44] Hiervoor dient vooraf toestemming te worden gevraagd aan de rechtbank Den Haag.[45] Het concept-wetsvoorstel definieert wie als bron moet worden gezien. Dit zijn personen die gegevens ter openbaarmaking aan een journalist hebben verstrekt onder de voorwaarde dat de verstrekking niet tot hen kan worden herleid.

Aandachtspunten

De CTIVD heeft zich in het verleden verschillende malen uitgesproken over het toepassen van bijzondere bevoegdheden tegen journalisten. De bijzondere inbreuk die hiermee gepaard gaat, beïnvloedt de noodzakelijkheids-, proportionaliteits- en subsidiariteitsweging.

De CTIVD heeft in haar toezichtsrapport nr. 10 aangegeven dat zij een kortere toestemmingstermijn aangewezen acht dan de wettelijke termijn van drie maanden, bijvoorbeeld van een maand.[46] De voorgestelde regeling kent geen kortere toestemmingstermijn. De CTIVD adviseert artikel 24, vijfde lid, van het concept-wetsvoorstel ook van toepassing te verklaren op de voorgestelde regeling.

Volgens het concept-wetsvoorstel is het aan de diensten vast te stellen dat sprake is van een journalist. De CTIVD vraagt zich af hoe de diensten dit kunnen vaststellen en hoe hier toezicht op kan worden uitgeoefend. Het criterium hiervoor is of een persoon zich beroepsmatig bezighoudt met het verzamelen, verspreiden of publiceren van informatie. In bepaalde gevallen zal niet direct duidelijk zijn dat de diensten met een journalist te maken hebben. Indien de diensten (ten onrechte) concluderen dat geen sprake is van een journalist zal ook de voorafgaande toetsing achterwege blijven. De CTIVD acht het aangewezen dat ook in gevallen van twijfel de diensten de voorgestelde regeling toepassen.

Eenzelfde soort aandachtspunt ligt wat de CTIVD betreft bij de definiëring van het begrip bron. De regeling is van toepassing indien een bron gegevens heeft verschaft onder de voorwaarde dat deze niet tot hem kunnen worden herleid. Het is de vraag hoe de diensten moeten weten dat aan de bron een dergelijke toezegging is gedaan door de journalist. Is de regeling niet van toepassing indien de journalist uit eigen beweging anonimiteit toezegt aan zijn bron? Volgens de CTIVD moet altijd als uitgangspunt worden gehanteerd dat de bron anoniem wenst te blijven en van een toezegging van de journalist aan zijn bron moet worden uitgegaan. Slechts bij concrete aanwijzingen van het tegendeel kan dit anders zijn.

---

[44] In een eerder stadium is een separaat wetsvoorstel ingediend waarin deze regeling is opgenomen. In het wetsvoorstel wordt voor een nadere toelichting hiernaar verwezen.

[45] Zie hoofdstuk 1, paragraaf 1.2.2, voor het advies van de CTIVD ten aanzien van *ex ante* toetsing.

[46] Toezichtsrapport van de CTIVD nr. 10 inzake het onderzoek van de AIVD naar het uitlekken van staatsgeheimen, *Kamerstukken II* 2006/07, 29 876, nr. 19 (bijlage), beschikbaar op www.ctivd.nl.

Het concept-wetsvoorstel schrijft een voorafgaande toets van de rechtbank Den Haag voor indien de uitoefening van de bijzondere bevoegdheid tegen een journalist is gericht op het achterhalen van een bron van de journalist. De journalistieke bronbescherming kan echter ook in het geding zijn indien de inzet van een bijzondere bevoegdheid niet is gericht op het achterhalen van een journalistieke bron.[47] Ook in deze gevallen kunnen bronnen van een journalist aan het licht komen. Gegevens die betrekking hebben op de identiteit van de bron van de journalist kunnen als zogenaamde bijvangst worden opgeslagen. Het is de vraag op welke wijze hierop toezicht kan worden gehouden. Het concept-wetsvoorstel regelt niets over deze situatie. De CTIVD adviseert het concept-wetsvoorstel op dit punt aan te scherpen.

De CTIVD merkt op dat het kabinet ook een aparte wettelijke voorziening wil treffen voor het tappen van advocaten.[48] Het is de CTIVD niet duidelijk waarom een dergelijke wettelijke voorziening niet ook zou moeten gelden voor het inzetten van bijzondere bevoegdheden ten aanzien van andere verschoningsgerechtigden (bijvoorbeeld artsen).

Advies

De CTIVD adviseert de toestemmingstermijn van een maand in artikel 24, vijfde lid, (toestemmingstermijn bij de inzet van bijzondere bevoegdheden ter ondersteuning van de taakuitvoering) van het concept-wetsvoorstel ook van toepassing te verklaren op artikel 25 lid 5 (journalisten).

De CTIVD adviseert het concept-wetsvoorstel op het punt van de toepassing van een bijzondere bevoegdheid tegen een journalist ook indien die niet is gericht op het achterhalen van een bron aan te scherpen.

3.5 Verkennen en binnendringen in geautomatiseerde werken (hacken)

[artikel 30; p. 51-55 MvT]

Concept-wetsvoorstel

De bevoegdheid tot hacken is in het concept-wetsvoorstel neergelegd in artikel 30. Het concept-wetsvoorstel verandert de hackbevoegdheid ten opzichte van de Wiv 2002 op enkele punten. De minister dient toestemming te verlenen voor alle gevallen waarin de hackbevoegdheid wordt toegepast. In de Wiv 2002 is dit toestemmingsniveau op het niveau van de dienst neergelegd. Het concept-wetsvoorstel voorziet ook in de bevoegdheid tot het verkennen van een geautomatiseerd werk. Hierbij wordt nog niet binnengedrongen in het geautomatiseerde werk. Het concept-wetsvoorstel voorziet tevens expliciet in de mogelijkheid via het geautomatiseerde werk van een derde binnen te dringen in het geautomatiseerde werk van het onderzoekssubject. Daarnaast legt het concept-wetsvoorstel expliciet de bevoegdheid vast technische voorzieningen in een geautomatiseerd werk aan te brengen ter ondersteuning van de uitvoering van andere bijzondere bevoegdheden.

---

[47] Zie bijvoorbeeld *Kamerstukken II* 2014/15, 34 032, nr. 3, p. 15-16. Dit betreft de memorie van toelichting bij het wetsvoorstel bronbescherming in strafzaken. Het wetsvoorstel merkt een journalist als beperkt verschoningsgerechtigde aan. Het wetsvoorstel voorziet niet enkel in het recht van de journalist zich te verschonen bij het zicht bieden op de identiteit van een journalistieke bron. Het wetsvoorstel voorziet ook in aanvullende waarborgen bij het inzetten van dwangmiddelen tegen journalisten in het algemeen.

[48] *Kamerstukken II* 2014/15, 29279, nr. 268.

Gegevens die zijn verkregen met de hackbevoegdheid moeten zo spoedig mogelijk maar uiterlijk binnen twaalf maanden op relevantie worden onderzocht.[49] Het concept-wetsvoorstel introduceert een medewerkingsplicht voor het ongedaan maken van de versleuteling van de gegevens. De medewerkingsplicht is gericht tot eenieder die kennis draagt van de wijze van versleuteling van gegevens opgeslagen of verwerkt op een geautomatiseerd werk.

Aandachtspunten

De CTIVD plaatst enkele kanttekeningen bij de bevoegdheid via het geautomatiseerde werk van een derde binnen te dringen in het geautomatiseerde werk van het onderzoekssubject (artikel 30, lid 1, onder b). Hiermee is in feite sprake van het toepassen van een bijzondere bevoegdheid tegen een non-target.[50] Dit is vergelijkbaar met het toepassen van een telefoontap tegen iemand in de omgeving van een target omdat het target zelf niet beschikt over een telefoon. De CTIVD heeft onder omstandigheden toegestaan dat een bijzondere bevoegdheid wordt ingezet tegen een non-target.[51] Hierbij komt wel extra gewicht toe aan het noodzakelijkheids-, proportionaliteits- en subsidiariteitsvereiste. Een non-target mag slechts dan het onderwerp van onderzoek zijn indien het redelijkerwijs niet mogelijk is op een andere wijze zicht te krijgen op het target.
Uit het concept-wetsvoorstel en de memorie van toelichting kan de CTIVD niet afleiden dat het binnendringen in het geautomatiseerde werk van een derde voor de diensten slechts mogelijk wordt geacht indien het target zelf onbereikbaar is. Het uitgangspunt zou moeten zijn dat het geautomatiseerde werk van het target het doelwit is. Volgens de CTIVD zou het concept-wetsvoorstel dit uitgangspunt expliciet moeten maken. Slechts in uitzonderingsgevallen kan hiervan worden afgeweken. In de aanvraag moet gemotiveerd worden aangegeven waarom hiertoe is overgegaan zodat deze overweging kan worden getoetst.

De CTIVD mist de noodzakelijke waarborgen die ervoor dienen te zorgen dat het binnendringen in het geautomatiseerde werk van een derde enkel dient om binnen te dringen in het werk van het onderzoekssubject. En dus bijvoorbeeld niet om te dienen als zelfstandige bron van informatie.

Advies

De CTIVD adviseert in artikel 30 aanvullende waarborgen op te nemen ten aanzien van het binnendringen in het geautomatiseerde werk van een derde.

---

[49] De CTIVD gaat in paragraaf 3.6.1 in op de bewaartermijn van twaalf maanden.

[50] Een target is een onderzoekssubject van de AIVD of de MIVD. Een non-target is een persoon of organisatie via wie of via welke de dienst informatie probeert te achterhalen over een target.

[51] Toezichtsrapport van de CTIVD 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), *Kamerstukken II* 2008/09, 29 924, nr. 29 (bijlage), § 6.2.2, beschikbaar op www.ctivd.nl.

3.6 Bewaartermijnen voor verzamelde gegevens

[artikelen 30, 32 en 38; p. 51-55, 57-62, 85-87 MvT]
[artikel 33; p. 62-69 MvT]

3.6.1 Bewaartermijnen voor door de diensten verworven communicatie

Concept-wetsvoorstel
Er zijn twee verschillende bewaartermijnen voor verworven communicatie opgenomen in het concept-wetsvoorstel:

- Gegevens die zijn verkregen door de uitoefening van een gerichte bevoegdheid moeten zo spoedig mogelijk op hun relevantie voor het onderzoek waarvoor ze zijn verworven worden onderzocht. Gegevens waarvan is vastgesteld dat deze niet relevant zijn voor het onderzoek dan wel niet op hun relevantie voor het onderzoek zijn onderzocht, worden na een periode van ten hoogste 12 maanden vernietigd. Deze bewaartermijn is opgenomen in de voorgestelde artikelen 30 (hacken), 32 (gerichte interceptie) en 38 (opvragen opgeslagen gegevens). Het concept-wetsvoorstel geeft de diensten een jaar de tijd om verzamelde gegevens op relevantie te beoordelen.
- Gegevens die zijn verzameld door uitoefening van de bevoegdheid van artikel 33 lid 1 (grootschalige interceptie) mogen voor een periode van ten hoogste drie jaar na verwerving worden bewaard ten behoeve van onderzoek aan gegevens (search), metadata-analyse en selectie van de gegevens (zie **paarse blok** in het schema in hoofdstuk 2, paragraaf 2.3.1). In de memorie van toelichting is opgenomen dat de huidige bewaartermijn van één jaar al lange tijd als een groot knelpunt wordt ervaren. De CTIVD heeft deze problematiek ook gesignaleerd in haar toezichtsrapport nr. 5a uit 2005.[52]

Aandachtspunten
De CTIVD acht het van belang dat de wet maximum bewaartermijnen stelt. Na verloop van deze termijn dienen gegevens te worden vernietigd. De bewaartermijnen moeten concreet worden aangemerkt, bijvoorbeeld in een aantal maanden of een jaar. Het gebruik van open normen (bijvoorbeeld, 'zo spoedig mogelijk' of 'binnen een redelijke termijn') verdient hierbij volgens de CTIVD niet de voorkeur. De bescherming van de persoonlijke levenssfeer vraagt om een korte bewaartermijn die niet langer is dan strikt noodzakelijk.

Het belang van deze waarborg kwam ook tot uiting in de uitspraak van het Hof van Justitie van de Europese Unie van 8 april 2014. Het Hof heeft in deze uitspraak de richtlijn betreft gegevensbewaring (ook wel genoemd de Dataretentierichtlijn) ongeldig verklaard. Het Hof achtte hierbij onder meer van belang dat bewaartermijnen niet langer mogen zijn dan strikt noodzakelijk. Waarom de bewaartermijn niet korter kan zijn, dient te worden gemotiveerd op basis van objectieve criteria.53 De richtlijn bood op dit punt onvoldoende duidelijkheid. De CTIVD weegt deze uitspraak mee bij haar beoordeling van het concept-wetsvoorstel.

De termijn van twaalf maanden voor de bewaring van gericht verzamelde gegevens acht de CTIVD lang. De motivering in de memorie van toelichting voor de lengte van de bewaartermijn overtuigt niet. Duidelijk moet worden op basis van welke objectieve criteria deze termijn strikt noodzakelijk is.

---

[52] Toezichtsrapport van de CTIVD nr. 5a inzake de rechtmatigheid van het MIVD-onderzoek naar proliferatie van massavernietigingswapens en overbrengingsmiddelen, geen kamerstuk, beschikbaar op www.ctivd.nl.

[53] Hof van Justitie van de Europese Unie, 8 april 2014, zaken C2-93/12 en C-594/12, r.o. 63-64.

Met name bij de hackbevoegdheid en de bevoegdheid tot het opvragen van opgeslagen gegevens zullen relatief veel gegevens worden verkregen van 'onschuldige burgers'. Die gegevens zouden sneller moeten worden vernietigd dan pas na een jaar. De omstandigheid dat de diensten nog geen kennis hebben genomen van deze gegevens en de inbreuk op de privacy daardoor beperkt is, acht de CTIVD niet voldoende voor het hanteren van een lange bewaartermijn. De opslag van deze gegevens door de diensten leidt op zichzelf immers al tot een inbreuk op de persoonlijke levenssfeer.

Volgens de CTIVD dient vernietiging van gegevens waarvan is vastgesteld dat deze niet relevant zijn, direct te gebeuren. Het concept-wetsvoorstel staat toe dat ook de vastgestelde niet-relevante gegevens maximaal twaalf maanden bewaard mogen blijven.

Het concept-wetsvoorstel geeft een termijn van drie jaar voor de bewaring van verworven communicatie in andere gevallen (grootschalig geïntercepteerde communicatie). Deze termijn acht de CTIVD zeer lang. Het gaat om communicatie die in bulk wordt verworven. De verwerving is in deze fase nog niet gericht op communicatie van personen en organisaties maar bijvoorbeeld op het intercepteren van kabelgebonden communicatie uit een bepaald land of regio. De aard en omvang van de verwerving is dusdanig dat naar verwachting het merendeel van de gegevens die worden verworven niet relevant zijn voor enig onderzoek van de diensten.

De motivering in de memorie van toelichting voor de lengte van de bewaartermijn overtuigt niet. Duidelijk moet worden op basis van welke objectieve criteria deze termijn strikt noodzakelijk is. De memorie van toelichting geeft aan dat een periode van één jaar al geruime tijd als problematisch wordt ervaren. Een korte bewaartermijn zou een doeltreffende analyse van data in de weg staan. Dit acht de CTIVD op zichzelf niet redengevend. Het geeft slechts aan dat bewaring op zichzelf noodzakelijk is. Indien niet met objectieve criteria kan worden onderbouwd waarom verlenging van de bewaartermijn strikt noodzakelijk is, adviseert de CTIVD de bewaartermijn op één jaar te houden.

Het is de CTIVD ook uit haar toezichthoudende taak niet gebleken dat de huidige termijn problematisch is. In haar toezichtsrapport nr. 5a (2005) heeft de CTIVD weliswaar beschreven dat zij het standpunt (van de MIVD) dat de bewaartermijn dient te worden verruimd begrijpelijk achtte maar tekende daarbij aan dat zij in het enkele opslaan van de gegevens nog geen inbreuk op de privacy van betrokken personen zag.[54] Gelet op de ontwikkelingen in de jurisprudentie en technologie sindsdien is de CTIVD nu van oordeel dat dit standpunt dient te worden verlaten. De MIVD heeft in het kader van toezichtsrapport 5a opgemerkt dat voorkomen dient te worden dat mogelijk waardevolle inlichtingen, die relevant kunnen zijn voor enig (lopend) onderzoek, vernietigd zouden worden. De CTIVD merkt daarover nu op dat het vaststellen van harde bewaar- en vernietigingstermijnen altijd het risico met zich meebrengt dat waardevolle inlichtingen verloren gaan. Dit risico moet echter worden afgewogen tegen het belang van de bescherming van de persoonlijke levenssfeer. Dit laatste belang is geen statisch gegeven en wordt onder meer beïnvloed door technologische ontwikkelingen. Deze stellen de diensten in staat veel meer (ook niet relevante) informatie te halen uit opgeslagen data. Dit dient van invloed te zijn op de lengte van de bewaartermijn.[55]

---

[54] Zie toezichtsrapport 5a inzake het MIVD-onderzoek naar proliferatie van massavernietigingswapens en overbrengingsmiddelen, paragraaf 4.2.5, beschikbaar op www.ctivd.nl.

[55] Voor een vergelijkbare afweging, zie de korte bewaartermijn voor celmateriaal in het kader van DNA-onderzoek. Ook daar zijn de technologische ontwikkelingen van belang. Doordat steeds meer mogelijk is met kleine hoeveelheden celmateriaal is een korte bewaartermijn aangewezen.

Volgens de CTIVD dient de bewaartermijn in te gaan op het moment van verwerving. Het enkele opslaan van telecommunicatie levert al een inbreuk op de persoonlijke levenssfeer op. Dat hiervan nog geen kennis is of kan worden genomen, is hierbij niet van belang. Om die reden ziet de CTIVD geen reden de bewaartermijn pas in te laten gaan na het ontsleutelen van de gegevens. De CTIVD adviseert het voorstel zodanig aan te passen dat de bewaartermijn ingaat op het moment van verwerving.

Advies

De termijn van twaalf maanden voor de bewaring van gericht verzamelde gegevens acht de CTIVD lang. De motivering in de memorie van toelichting voor de lengte van de bewaartermijn overtuigt niet. De CTIVD adviseert om in de memorie van toelichting duidelijk te maken op basis van welke objectieve criteria de voorgestelde termijn strikt noodzakelijk is.

De CTIVD adviseert dat vernietiging van gericht verzamelde gegevens waarvan is vastgesteld dat deze niet relevant zijn direct plaatsvindt, en niet, zoals wordt voorgesteld, dat deze gegevens maximaal twaalf maanden mogen worden bewaard.

Het concept-wetsvoorstel geeft een termijn van drie jaar voor de bewaring van grootschalig geïntercepteerde communicatie. Deze termijn acht de CTIVD zeer lang. De motivering in de memorie van toelichting voor de lengte van de bewaartermijn overtuigt niet. De CTIVD adviseert om in de memorie van toelichting duidelijk te maken op basis van welke objectieve criteria de voorgestelde termijn strikt noodzakelijk is. Indien niet met objectieve criteria kan worden onderbouwd waarom verlenging van de bewaartermijn strikt noodzakelijk is, adviseert de CTIVD de bewaartermijn op één jaar te houden.

Tot slot adviseert de CTIVD het voorstel zodanig aan te passen dat de bewaartermijn voor grootschalig geïntercepteerde communicatie ingaat op het moment van verwerving.

3.6.2 Bewaartermijn voor DNA-profielen

[artikel 28; p. 46-49 MvT]

Concept-wetsvoorstel

Artikel 28 voorziet in een expliciete regeling voor DNA-onderzoek. Het geeft de diensten de mogelijkheid DNA-onderzoek te verrichten ter vaststelling van de identiteit. Hieronder valt ook de verificatie van de identiteit van een persoon. Uit de memorie van toelichting volgt dat gezondheidsonderzoek niet is toegestaan.

De resultaten van DNA-onderzoek mogen slechts worden gebruikt voor het onderzoek waarvoor de toestemming is verleend. Verdere verwerking (zowel intern als extern) is slechts toegestaan na toestemming van de minister.

Het concept-wetsvoorstel stelt bewaar- en vernietigingstermijnen voor het bewaren van celmateriaal en DNA-profielen. Nadere regels voor het verwerken van DNA-profielen zullen worden gesteld bij algemene maatregel van bestuur (AMvB).

Aandachtspunten
De bewaartermijn voor celmateriaal (maximaal drie maanden) gaat in na het verrichten van DNA-onderzoek. Er is echter geen termijn gesteld waarbinnen het DNA-onderzoek dient te zijn verricht. De CTIVD acht het aangewezen een bewaartermijn vast te leggen die ingaat direct na de verwerving van het celmateriaal dan wel een concrete termijn te stellen waarbinnen het DNA-onderzoek moet worden verricht. Deze bewaartermijn moet zo kort mogelijk zijn gelet op de grote hoeveelheid genetische en gezondheidsgerelateerde informatie die besloten ligt in celmateriaal. De bewaartermijn mede afhankelijk stellen van het verrichten van DNA-onderzoek acht de CTIVD niet juist.

Voor het bewaren van DNA-profielen is een bewaartermijn in het concept-wetsvoorstel opgenomen van ten hoogste vijf jaar. Uit de memorie van toelichting blijkt niet waar deze termijn op is gebaseerd.

Advies
De CTIVD adviseert nader toe te lichten waarom een bewaartermijn van vijf jaar voor DNA-profielen strikt noodzakelijk wordt geacht en niet met een kortere termijn kan worden volstaan.

Zij adviseert voorts de bewaartermijn voor celmateriaal in te laten gaan op het moment van verwerving.

3.7 Geautomatiseerde data-analyse

[artikel 47; p. 101-103 MvT]

Concept-wetsvoorstel
Artikel 47 voorziet in een expliciete wettelijke grondslag voor geautomatiseerde data-analyse als werkmethode voor de diensten. Deze bepaling is niet onder het regime van bijzondere bevoegdheden gebracht.

Aandachtspunten
Net als bij metadata-analyse waarvoor in het voorstel ministeriële toestemming is vereist, kunnen ook bepaalde vormen van geautomatiseerde data-analyse die de inhoud van de gegevens betreffen zijn gericht op het identificeren van personen en organisaties of op het onderkennen van bepaalde patronen, waardoor inbreuk wordt gemaakt op de persoonlijke levenssfeer. In het voorgestelde artikel 47 is hier geen regeling voor getroffen. Het opnemen van een dergelijke regeling in het hoofdstuk bijzondere bevoegdheden ligt voor de hand.

Advies
De CTIVD adviseert, net als bij metadata-analyse, een regeling te treffen voor die gevallen van geautomatiseerde data-analyse waardoor inbreuk wordt gemaakt op de persoonlijke levenssfeer.

3.8 Het bevorderen of treffen van maatregelen door de diensten

[artikel 61; p. 119-121 MvT]

Concept-wetsvoorstel

In het concept-wetsvoorstel krijgen de diensten een separate bijzondere bevoegdheid tot het bevorderen en treffen van maatregelen ter bescherming van de door de diensten te behartigen belangen (artikel 61). Dit betreft een uitbreiding ten opzichte van de huidige wet, want deze bevoegdheid is nu enkel onderdeel van de bevoegdheid tot het inzetten van een agent (artikel 21 lid 1 aanhef en onder a Wiv 2002).

Aandachtspunten

Ten eerste wordt met deze uitbreiding mogelijk gemaakt dat behalve agenten ook andere personen belast kunnen worden met handelingen die (medewerking aan) een strafbaar feit kunnen inhouden. Het ligt in de rede, zoals ook in de memorie van toelichting wordt aangehaald, dat het hier (naast agenten) gaat om reguliere medewerkers van de diensten. Artikel 61 (in samenhang met artikel 26) van het concept-wetsvoorstel beperkt zich echter niet daartoe; strikt genomen kan iedereen in beginsel door de dienst worden belast met het plegen van strafbare feiten zonder dat er sprake is van het zijn van agent of medewerker van de dienst.

Volgens de memorie van toelichting bij het concept-wetsvoorstel ziet de bevoegdheid bovendien niet alleen op het verstoren van activiteiten, maar ook op maatregelen in de preventieve sfeer.[56] Als voorbeelden worden genoemd het onder controle houden en krijgen van targets en het scheppen van voorwaarden om op een effectievere manier bijzondere bevoegdheden te kunnen toepassen. Uitdrukkelijk wordt gesteld dat deze bevoegdheid niet bedoeld is als ultimum remedium. Blijkens de memorie van toelichting bij artikel 21 van de huidige wet is deze bevoegdheid (oorspronkelijk) wel zo bedoeld.[57]

Tot slot wordt in het eerste lid van artikel 61 van het concept-wetsvoorstel bepaald dat het bevorderen en treffen van maatregelen kan plaatsvinden met behulp van een technisch hulpmiddel. In de memorie van toelichting bij het concept-wetsvoorstel wordt hierover slechts vermeld dat het feit dat van deze hulpmiddelen gebruik mag worden gemaakt buiten kijf wordt gesteld. Het concept-wetsvoorstel geeft hiermee onvoldoende duidelijk aan of de inzet van een dergelijk hulpmiddel op grond van deze bevoegdheid kan leiden tot een inbreuk op grondrechten van personen zoals het recht op bescherming van de persoonlijke levenssfeer.

---

[56] Zie memorie van toelichting, p. 119-121.

[57] Zie *Kamerstukken II* 1997/98, 25 877, nr. 3, p. 34, *Kamerstukken II* 1999/2000, 25 877, nr. 8, p. 61 en *Kamerstukken II* 2000/01 25 877, nr. 59, p. 9 en 10.

Advies
Gezien het afbreukrisico van het op instructie van de diensten plegen van handelingen die (medewerking aan) een strafbaar feit kunnen inhouden, adviseert de CTIVD de kring van personen die hiervoor in aanmerking komt in de wet te beperken.

Daarnaast adviseert de CTIVD in de memorie van toelichting bij het concept-wetsvoorstel aan te geven waarom het noodzakelijk wordt geacht de toepassing van de bevoegdheid tot het bevorderen of treffen van maatregelen niet langer slechts als *ultimum remedium* te kunnen inzetten en in hoeverre de inzet van een technisch hulpmiddel al dan niet kan leiden tot een inbreuk op het recht op bescherming van de persoonlijke levenssfeer.

3.9 Samenwerking met buitenlandse diensten

[artikelen 76-78; p. 136-144 MvT]

3.9.1 Toestemming voor het aangaan van samenwerkingsrelaties

Concept-wetsvoorstel
Artikel 76 van het voorstel bepaalt dat er eerst een afweging moet plaatsvinden aan de hand van drie criteria (democratische inbedding, respect voor mensenrechten en professionaliteit en betrouwbaarheid) voordat een samenwerkingsrelatie met een buitenlandse inlichtingen- of veiligheidsdienst mag worden aangegaan. De afweging dient mede de aard en de intensiteit van de beoogde samenwerking te omvatten. In de memorie van toelichting wordt uitgelegd dat daarbij moet worden gedacht aan zaken als ten aanzien van welke onderwerpen onder welke omstandigheden gegevensuitwisseling kan plaatsvinden en aan welke andere voorwaarden moet worden voldaan.

In het concept-wetsvoorstel is ervoor gekozen de toestemming voor het aangaan van een samenwerkingsrelatie met een buitenlandse inlichtingen- en/of veiligheidsdienst te beleggen bij de minister (artikel 76 lid 4). De bevoegdheid kan echter gemandateerd worden aan het hoofd van de dienst, die dan wel de minister daarvan zo spoedig mogelijk op de hoogte moet stellen. Daarover staat in de memorie van toelichting 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. Aangegeven wordt dat wel aanvullend in de mogelijkheid is voorzien dat de minister de bevoegdheid tot het verlenen van toestemming aan het hoofd van de dienst mandateert. De minister dient in een dergelijk geval terstond van een verleende toestemming op de hoogte te worden gesteld.[58]

[58] Voorstel van Wet op de inlichtingen- en veiligheidsdiensten 20XX; memorie van toelichting (consultatieversie juni 2015), p. 140.

Aandachtspunten
De CTIVD ziet het als een belangrijke waarborg dat de minister zelf altijd toestemming geeft voor het aangaan van een samenwerkingsrelatie. Het gaat om meer dan alleen een akkoord voor het aangaan van een nieuwe relatie – op zichzelf ook een belangrijke afweging – maar ook om de gegevens die binnen die samenwerking mogen worden uitgewisseld. Deze waarborg wordt uitgehold als de toestemming aan het hoofd van de dienst mag worden gemandateerd.

Advies
De CTIVD adviseert in de concept-wetsvoorstel mandaat aan het hoofd van de dienst uit te sluiten.

3.9.2 Factoren die betrokken moeten worden bij de afweging

Concept-wetsvoorstel
De memorie van toelichting bij het concept-wetsvoorstel gaat uitgebreid in op de inhoud van de afweging die de dienst moet maken aan de hand van de eerdergenoemde drie criteria, voordat een samenwerkingsrelatie met een buitenlandse dienst mag worden aangegaan. Onder de drie criteria (1) democratische inbedding, (2) respect voor mensenrechten en (3) professionaliteit en betrouwbaarheid, worden verschillende factoren gebracht.

De CTIVD leidt uit de memorie van toelichting af dat deze factoren allemaal separaat worden gewogen in de afweging die de dienst maakt. Het gaat onder andere om het beantwoorden van de volgende vragen:

- In hoeverre geeft deze buitenlandse dienst inzicht in zijn taken, bevoegdheden en werkwijze? (het gaat hier om de transparantie van die dienst)[59]
- Heeft het desbetreffende land mensenrechtenverdragen geratificeerd en worden deze verdragen in de praktijk nageleefd?
- Wordt de buitenlandse dienst in verband gebracht met schendingen van mensenrechten in onderzoeken en rapporten van nationale en internationale mensenrechtenorganisaties?
- Welke ervaringen zijn opgedaan in het verleden met deze buitenlandse dienst?
- Hoe zijn de ervaringen van andere buitenlandse collega-diensten met deze buitenlandse dienst?

Aandachtspunten
Naast deze factoren, acht de CTIVD het van belang dat zoveel mogelijk zicht wordt verkregen op de manier waarop door een ontvangende buitenlandse dienst omgegaan zal worden met ongeëvalueerde gegevens. De verstrekking van deze gegevens is gevoelig vanuit het oogpunt van de bescherming van de persoonlijke levenssfeer, omdat nog niet is vastgesteld of de gegevens relevant zijn in relatie tot de taakuitvoering van de AIVD of de MIVD. Per definitie bevinden zich onder deze gegevens ook de persoonsgegevens van personen die geen relevantie hebben voor de nationale veiligheid. Bovendien gaat het bij ongeëvalueerde gegevens vaak om grote hoeveelheden (bulk).

[59] In haar toezichtsrapport nr. 38 inzake gegevensverwerking op het gebied van telecommunicatie door de AIVD en de MIVD heeft de CTIVD aanbevolen dat samenwerkingsrelaties mede worden beoordeeld op transparantie.

Deze overwegingen maken het in de ogen van de CTIVD belangrijk dat bij de afweging van de samenwerkingscriteria expliciet aandacht wordt besteed aan de manier waarop de verwerking, opslag en vernietiging van gegevens is vormgegeven bij een ontvangende dienst en de waarborgen die hierbij gelden. Het is vanuit de privacybescherming bijvoorbeeld essentieel dat ook een ontvangende dienst de verplichting heeft het irrelevante materiaal te vernietigen zodra dit mogelijk is.[60]

Advies
De CTIVD adviseert in de memorie van toelichting op te nemen dat bij de beoordeling van de samenwerkingscriteria expliciet aandacht moet worden besteed aan de waarborgen op het gebied van gegevensverwerking, opslag van gegevens en vernietiging van gegevens bij de ontvangende buitenlandse dienst.

3.9.3 De verstrekking van persoonsgegevens aan buitenlandse diensten

Concept-wetsvoorstel
Zoals hierboven al is benoemd, schrijft het concept-wetsvoorstel voor dat bij de afweging die voorafgaand aan het aangaan van een samenwerkingsrelatie met een buitenlandse dienst plaatsvindt, wordt aangegeven wat de aard en intensiteit van de beoogde samenwerking kan zijn. Dit houdt in dat ook wordt bepaald ten aanzien van welke onderwerpen onder welke omstandigheden gegevensuitwisseling kan plaatsvinden. Over het verstrekken van persoonsgegevens wordt in de memorie van toelichting aangegeven dat hieraan uitdrukkelijk aandacht moet worden besteed bij de afweging. Er staat dat bij risicodiensten van oudsher terughoudendheid wordt betracht bij het uitwisselen van persoonsgegevens. Het uitgangspunt blijft dat op voorhand geen samenwerking kan worden uitgesloten. Volgens de memorie van toelichting vindt bij de diensten die de mensenrechten onvoldoende respecteren een uitdrukkelijke weging plaats aan de hand van de zwaarte van het belang dat met – een bepaalde vorm van – samenwerking is gemoeid.[61]

Dit vormt derhalve een integraal onderdeel van hetgeen aan de minister moet worden voorgelegd voorafgaand aan het aangaan van een nieuwe samenwerkingsrelatie. Voor het verstrekken van persoonsgegevens in individuele gevallen is op grond van het voorstel geen ministeriële toestemming vereist.[62]

Aandachtspunten
De CTIVD is er een voorstander van dat aan de voorkant een gedegen afweging wordt gemaakt aan de hand van de samenwerkingscriteria, die ook te gelden heeft als kader voor de invulling van de relatie. Zij wijst er echter op dat als de mogelijkheid om persoonsgegevens te verstrekken aan een risicodienst[63] open wordt gelaten bij deze voorafgaande beoordeling, het aan de dienst wordt overgelaten om te beslissen of in een individueel geval persoonsgegevens kunnen worden verstrekt. Hiervoor is dan intern toestemming vereist.

---

60 De regelgeving in het Verenigd Koninkrijk verplicht ook tot een dergelijke beoordeling voordat metadata (ongeëvalueerde gegevens) wordt verstrekt *(Acquisition and disclosure of communications data Code of Conduct*, para 7.18).

61 Voorstel van Wet op de inlichtingen- en veiligheidsdiensten 20XX; memorie van toelichting (consultatieversie juni 2015), p. 139-140.

62 Althans, voor zover het gaat om geëvalueerde gegevens. Voor het verstrekken van ongeëvalueerde gegevens is wel toestemming van de minister vereist (art. 49 lid 3 en art. 77 lid 2 concept-wetsvoorstel).

63 Een dienst die niet voldoet aan de samenwerkingscriteria, waaronder respect voor mensenrechten.

Het verstrekken van persoonsgegevens aan een risicodienst is bij uitstek een activiteit die ernstige gevolgen met zich mee kan brengen voor de betrokkene. Welke afspraken ook worden gemaakt met de buitenlandse dienst en welke voorwaarden ook worden verbonden aan de verstrekking, feit blijft dat de gegevens zijn overgedragen aan een buitenlandse staat die daarmee kan doen wat hij wil. De rapportages van mensenrechtenorganisaties zijn helder over de behandeling die een verdachte te wachten kan staan in bepaalde landen. Indien een fair trial ontbreekt, is het bovendien mogelijk dat gegevens die de AIVD of de MIVD heeft verstrekt over een persoon weinig tegenspraak meer ondervinden en daardoor een zwaarder gewicht krijgen in een gerechtelijke procedure dan in Nederland het geval zou zijn.

In het licht van de risico's die de verstrekking van persoonsgegevens met zich mee kunnen brengen, vindt de CTIVD dat aanvullende waarborgen noodzakelijk zijn. Ten eerste zou ten behoeve van de zorgvuldigheid de verstrekking van deze gegevens uitsluitend schriftelijk moeten plaatsvinden, zodat interne controle en extern toezicht hierop mogelijk is. Dit biedt ook de mogelijkheid bij de verstrekking van gegevens schriftelijk aanvullende voorwaarden op te nemen die zien op het gebruik van de gegevens (bijvoorbeeld: de gegevens mogen niet gebruikt worden in een gerechtelijke procedure).

Ten tweede acht de CTIVD de waarborg van ministeriële toestemming in plaats van interne toestemming per verstrekking van persoonsgegevens aan een risicodienst op zijn plaats. Per geval zou op het niveau van de minister moeten worden beoordeeld of de reden voor de verstrekking van de gegevens opweegt tegen de mogelijke gevolgen voor de betrokkene. Bij deze afweging moet de aard van de gegevens worden betrokken en (indien van toepassing) het soort mensenrechtenschendingen waarmee de dienst in verband wordt gebracht. Ook zijn praktische aspecten relevant, zoals de vraag of de betrokkene zich in het desbetreffende land bevindt of daar naar verwachting naartoe zal reizen. Deze afweging zou schriftelijk moeten worden vastgelegd. De CTIVD is zich ervan bewust dat zij eerder heeft aanbevolen de toestemming voor het verstrekken van persoonsgegevens aan risicodiensten op het niveau van het diensthoofd te beleggen. De reden om nu toestemming op het niveau van de minister voor te stellen is dat het past in de structuur van het concept-wetsvoorstel om ministeriële toestemming te vereisen waar de verstrekking van gegevens aan buitenlandse diensten een hoger risico met zich meebrengt dan gebruikelijk (bijvoorbeeld het verstrekken van ongeëvalueerde gegevens). Dat geldt zeker ook voor het verstrekken van persoonsgegevens aan risicodiensten.

De CTIVD merkt hierbij op dat de praktijkgevallen van verstrekking van persoonsgegevens aan risicodiensten die zij in het kader van klachten heeft onderzocht in de afgelopen jaren haar hebben gesterkt in haar overtuiging dat de waarborgen op dit punt moeten worden aangescherpt. Zonder deze waarborgen ziet zij niet in hoe Nederland kan voldoen aan zijn mensenrechtelijke verplichtingen.

Advies

De CTIVD adviseert in artikel 77 een bepaling op te nemen inhoudende dat voor de verstrekking van persoonsgegevens aan buitenlandse diensten die niet voldoen aan de samenwerkingscriteria, per verstrekking toestemming van de minister benodigd is. Zij adviseert ook in de wetstekst op te nemen dat deze verstrekking uitsluitend schriftelijk dient plaats te vinden.

3.9.4 Het verlenen van ondersteuning aan buitenlandse diensten

Concept-wetsvoorstel

In artikel 77 leden 4 t/m 6 van het concept-wetsvoorstel wordt de verlening van ondersteuning aan buitenlandse inlichtingen- en veiligheidsdiensten geregeld. Uit de leden 5 en 6 blijkt dat toestemming van de minister vereist is voor deze vorm van samenwerking. Wel kan de bevoegdheid worden gemandateerd aan het hoofd van de dienst, voor zover het niet om een risicodienst gaat. In de memorie van toelichting wordt onder meer opgemerkt dat indien het verzoek om toestemming tevens betekent dat de inzet van bijzondere bevoegdheden plaatsvindt door de dienst (AIVD/MIVD), het regulier toestemmingsregime voor dit laatste blijft gelden.

Aandachtspunten

Een thema dat in een aantal rapporten van de CTIVD terugkeert, is de inhoud van de afweging die gemaakt dient te worden als de AIVD of de MIVD een bijzondere bevoegdheid inzet op verzoek van een buitenlandse dienst. Vooral de noodzakelijkheidstoets is dan problematisch. De vraag die hier voor de hand ligt is: hoe kan de inzet noodzakelijk zijn in het kader van de eigen inlichtingen- en veiligheidstaken van de AIVD of MIVD als die inzet uitsluitend in het belang van de buitenlandse dienst plaatsvindt? Een volledige noodzakelijkheidstoets lijkt niet mogelijk. De visie van de CTIVD is dat deze noodzakelijkheid in dergelijke situaties deels kan worden ingevuld door de wettelijke plicht van de AIVD en de MIVD goede verbindingen te onderhouden met buitenlandse diensten. Voor dat doel kan het noodzakelijk zijn bijzondere bevoegdheden in te zetten. Dit op zichzelf is echter niet voldoende. De AIVD en de MIVD hebben daarnaast ook een eigen verantwoordelijkheid nadere tekst en uitleg te vragen aan de verzoekende buitenlandse dienst, zodat aan de hand daarvan de noodzaak van de inzet voor die dienst tot op zekere hoogte kan worden beoordeeld.[64] De CTIVD acht het van belang dat de memorie van toelichting duidelijkheid schept ten aanzien van de inhoud van de afweging. Zonder een heldere visie op wat er precies dient te worden afgewogen is het toepassen van het regulier toestemmingsregime een lege dop. De CTIVD heeft in dit opzicht dan ook geen houvast voor het uitoefenen van toezicht.

Advies

De CTIVD adviseert in de memorie van toelichting nader in te gaan op de inhoud van de toets die moet worden verricht als de AIVD en/of de MIVD een bijzondere bevoegdheid inzet ten behoeve van een buitenlandse dienst.

3.10 Conclusie

De CTIVD heeft in dit hoofdstuk onderzocht waar adequate waarborgen voor de privacy in het concept-wetsvoorstel nog ontbreken. Zij komt tot de conclusie dat het wetsvoorstel op dit punt op verschillende onderdelen tekort schiet, zoals bij de uitbreiding van de hackbevoegdheid en bij de lengte van de bewaartermijnen voor verzamelde gegevens.

[64] Zie juridische bijlage van toezichtsrapport nr. 22b inzake de samenwerking van de MIVD met buitenlandse inlichtingen- en/of veiligheidsdiensten, *Kamerstukken II* 2014/15, 29 924, nr. 128 (bijlage), beschikbaar op www.ctivd.nl.

4 Overige onderwerpen

4.1 Inleiding

In dit hoofdstuk behandelt de CTIVD een aantal overige onderwerpen. De punten die de CTIVD hierbij aandraagt zien slechts op de formulering en vormgeving van bepalingen in het concept-wetsvoorstel.

Hier wil de CTIVD er op wijzen dat zij in de praktijk al enige tijd de volgende naam hanteert: Commissie van Toezicht *op* de inlichtingen- en veiligheidsdiensten. Dit vindt zij toegankelijker dan het wat ouderwetse woord 'betreffende'. In het wetsvoorstel (artikel 85 lid 1) en de memorie van toelichting wordt nog verwezen naar de Commissie van Toezicht *betreffende* de inlichtingen- en veiligheidsdiensten. De CTIVD verzoekt haar naam aan te passen op dit onderdeel.

4.2 Ontheffing van wettelijke voorschriften voor gegevensverstrekking van agenten

[artikelen 22 en 26; p. 24-28 en p. 39-43 MvT]

Concept-wetsvoorstel
In artikel 22 lid 4 van het concept-wetsvoorstel wordt, net zoals in de huidige wet, bepaald dat de voor een "verantwoordelijke voor een gegevensverwerking" geldende wettelijke voorschriften niet van toepassing zijn indien deze als informant gegevens aan de diensten verstrekt.

Aandachtspunten
In haar toezichtsrapport nr. 39 trekt de CTIVD de conclusie dat de ontheffing van andere wettelijke verplichtingen (bijvoorbeeld op het gebied van de bescherming van persoonsgegevens) die geldt voor informanten van de dienst wanneer zij gegevens aan de dienst verstrekken, ook van toepassing moet worden geacht op agenten.[65] Dit is logisch gezien het feit dat de inzet van een agent feitelijk een 'zwaardere' bevoegdheid is dan het bevragen van een informant.

Advies
De CTIVD adviseert in artikel 26 vast te leggen dat eventuele wettelijke restricties niet gelden wanneer een agent gegevens verstrekt aan de dienst.

4.3 Ambtsberichten aan het OM en andere bestuursorganen

[artikelen 52 en 53; p. 110-112 MvT]

Concept-wetsvoorstel
De artikelen betreffende gegevensverstrekking aan het OM en aan andere, bij AMvB aangewezen bestuursorganen zijn niet gewijzigd ten opzichte van de huidige Wiv.

[65] Toezichtsrapport van de CTIVD inzake onderzoek door de AIVD op sociale media, *Kamerstukken II* 2013/14, 29 924, nr. 114 (bijlage), beschikbaar op www.ctivd.nl, para. 5.4.2.

Aandachtspunten
De CTIVD wijst erop dat in de eerste leden van de artikelen wordt gesproken van de verwerking van gegevens door of ten behoeve van de dienst waarvan "blijkt" (artikel 52 lid 1) of "is gebleken" (artikel 53 lid 1). Hier wordt de situatie beschreven waarin de diensten bij hun lopende onderzoeken op eigen initiatief gegevens signaleren die tevens van belang kunnen zijn voor de behartiging van de aan andere instanties opgedragen belangen. In de praktijk komt het in ieder geval bij ambtsberichten aan het OM regelmatig voor dat een verzoek vanuit het OM de aanleiding vormt voor het ambtsbericht. Dit neemt uiteraard niet weg dat het dient te gaan om gegevens die de dienst in het kader van zijn taakuitvoering (heeft) verwerkt. Ook bij gegevensverstrekking aan andere bestuursorganen dan het OM, op grond van een dringende en gewichtige reden, kan de CTIVD zich voorstellen dat de AIVD of de MIVD een ambtsbericht uitbrengt naar aanleiding van een verzoek daartoe. Een dergelijke situatie zou zich kunnen voordoen als een burgemeester de AIVD vraagt om nadere gegevens over een bepaalde groepering die een demonstratie heeft aangekondigd.

Advies
De CTIVD adviseert in de verwoording van artikel 52 lid 1 en artikel 53 lid 1 tot uitdrukking te brengen dat er ook sprake kan zijn van informatieverzoeken.

4.4 Technische en andere vormen van ondersteuning

[artikel 77; p. 142 MvT]

Concept-wetsvoorstel
In artikel 77 leden 4 t/m 6 van het concept-wetsvoorstel wordt de verlening van ondersteuning aan buitenlandse inlichtingen- en veiligheidsdiensten geregeld.

Aandachtspunten
Een onduidelijkheid die de CTIVD in haar rapporten heeft benoemd ten aanzien van het verlenen van (technische) ondersteuning aan buitenlandse diensten, is de reikwijdte van het begrip 'technische en andere vormen van ondersteuning'. In de memorie van toelichting bij de Wiv 2002 werd aangegeven dat het hierbij 'veelal' ging om de inzet van bijzondere bevoegdheden. Hieruit leidt de CTIVD af dat formeel ook andere vormen van ondersteuning onder de huidige bepaling vallen, zoals het geven van een training of het overdragen van technische kennis. Van de zijde van zowel de minister van BZK als de minister van Defensie is in reactie op dit standpunt aangegeven dat uitsluitend operationele ondersteuning onder deze bepaling dient te worden geschaard. De CTIVD heeft begrip voor het standpunt van de ministers dat het niet nodig is ministeriële toestemming te vereisen voor bijvoorbeeld het geven van een training aan een buitenlandse dienst.

Advies
De CTIVD adviseert om in de wetstekst van artikel 77 leden 4 t/m 6 nadrukkelijk aan te geven dat de regeling geldt voor operationele ondersteuning.

4.5 Behandeling van klachten

[Artikel 103; p. 164-166 MvT]

Concept-wetsvoorstel

In het concept-wetsvoorstel wordt de CTIVD als zelfstandige onafhankelijke klachtinstantie gepositioneerd die bindende oordelen kan geven. In het huidige stelsel vervult de CTIVD de rol van klachtenadviescommissie. De minister neemt na het advies van de CTIVD uiteindelijk een oordeel op de klacht, waarna de weg naar de Nationale ombudsman als externe klachtinstantie voor klager openstaat indien hij zich niet kan vinden in dit oordeel. De CTIVD komt in het voorgestelde systeem in de plaats van de Nationale ombudsman. De minister blijft verantwoordelijk voor de interne klachtprocedure die voorafgaand aan de externe procedure dient plaats te vinden.

Aandachtspunten

De CTIVD onderschrijft de gekozen positionering van de CTIVD als onafhankelijke externe klachtinstantie in het concept-wetsvoorstel. De invoering van een bindend klachtoordeel is conform de jurisprudentie van het EHRM over artikel 13 EVRM (effectief rechtsmiddel).[66] Deze regeling leidt op het gebied van klachtbehandeling dan ook tot de benodigde versterking van de effectiviteit van het (*ex post*) toezicht van de CTIVD.

De CTIVD ervaart een knelpunt in de wijze waarop thans in het concept-wetsvoorstel de interne klachtprocedure waarvoor de betrokken minister verantwoordelijk is, wordt gewaarborgd. In artikel 103 lid 3 wordt aangegeven dat de klager, alvorens zich tot de CTIVD te wenden, de betrokken minister in de gelegenheid stelt diens zienswijze op de klacht te geven. Naar het oordeel van de CTIVD komt met deze formulering onvoldoende tot uiting dat de minister verantwoordelijk is voor behandeling van de klacht in de interne klachtprocedure en over de klacht een oordeel dient te geven. In de memorie van toelichting bij het concept-wetsvoorstel wordt toegelicht dat de externe klachtprocedure bij de CTIVD dient te worden voorafgegaan door een interne klachtprocedure bij het bestuursorgaan zelf. Dit komt naar het oordeel van de CTIVD in het concept-wetsvoorstel onvoldoende tot uiting.

Advies

De CTIVD adviseert in artikel 103 een verwijzing op te nemen naar afdeling 9.1 van de Awb (bepalingen over de interne klachtprocedure).

[66] *Het mensenrechtenkader voor het Nederlandse stelsel van toezicht op de inlichtingen- en veiligheidsdiensten*, J.P. Loof, J. Uzman, T. Barkhuysen, A.C. Buyse, J.H. Gerards & R.A. Lawson, augustus 2015, te raadplegen via www.ctivd.nl, p. 11-13.

4.6 Beoordeling rechtmatigheid en behoorlijkheid

[Artikel 113; p. 165 MvT]

Concept-wetsvoorstel
In het concept-wetsvoorstel staat dat de afdeling klachtbehandeling van de CTIVD bij haar ingediende klachten beoordeelt op rechtmatigheid en behoorlijkheid.

Aandachtspunten
De CTIVD wijst er op dat klachtbehandeling gaat over behoorlijkheid. Hiermee onderscheid klachtbehandeling zich van rechtmatigheidstoezicht. Rechtmatigheid is een van de behoorlijkheidsnormen waaraan in klachtprocedures wordt getoetst. Het is niet conform het klachtrecht een van de behoorlijkheidsnormen afzonderlijk in de wet te benoemen.

Advies
De CTIVD adviseert in artikel 113 lid 1 de beoordeling van klachten alleen te richten op de behoorlijkheid.

4.7 Geheime informatie in bestuursrechtelijke en civielrechtelijke procedure

[artikelen 126 en 127; p. 170-175 MvT]

Concept-wetsvoorstel
Artikel 126 van het concept-wetsvoorstel regelt de procedure indien geheime informatie van de diensten in een bestuursrechtelijke procedure dient te worden ingebracht. De betrokken minister kan aan de bestuursrechter laten weten dat alleen de rechter van de stukken kennis kan nemen, met uitsluiting van de wederpartij of de partijen in het geding als de minister zelf geen procespartij is. De minister kan ook met een beroep op de geheimhouding van de informatie weigeren de gevraagde informatie te overleggen aan de bestuursrechter. Op grond van artikel 8:29 Awb beoordeelt de bestuursrechter of het beroep van de minister op het geheime karakter van de informatie terecht is. Artikel 126 van het concept-wetsvoorstel bepaalt dat de bestuursrechter de geheime stukken terug stuurt aan de betrokken minister indien hij van oordeel is dat het beroep op de geheimhouding niet gerechtvaardigd is. Op dit punt regelt het artikel wat thans al praktijk is.[67] De betrokken minister wordt hiermee in de gelegenheid gesteld zijn standpunt te heroverwegen en de informatie zonder voorbehoud ter beschikking te stellen.

Artikel 127 van het concept-wetsvoorstel bevat een vergelijkbare regeling voor civielrechtelijke procedures.

[67] Dit is nu opgenomen in de procesregeling van de ABRS.

Aandachtspunten

In artikel 126 eerste en tweede lid van het concept-wetsvoorstel is niet opgenomen het bepaalde in lid 5 van artikel 8:29, namelijk de procedure die moet worden gevolgd wanneer de bestuursrechter het beroep op de geheimhouding wel gerechtvaardigd vindt. In dat geval kan de bestuursrechter slechts met toestemming van partijen mede op grondslag van die geheime stukken uitspraak doen. Weliswaar wordt dit in de memorie van toelichting bij artikel 126 wel opgemerkt, maar het zou wenselijk zijn deze procedure ook in de Wiv vast te leggen. Evenmin is een verwijzing opgenomen naar het bepaalde van artikel 8:31 Awb. Dit artikel regelt wat er gebeurt indien de bestuursrechter van oordeel is dat het beroep op de geheimhouding van de stukken niet gerechtvaardigd is, maar de betrokken minister volhardt in zijn standpunt. In dat geval kan de rechter daaruit de gevolgtrekkingen maken die hem geraden voorkomen. Deze gevolgtrekking kan zijn: de gegrondheid van een beroep al dan niet gepaard met schadevergoeding. De memorie van toelichting verwijst weliswaar naar deze bepaling, maar het zou voor de duidelijkheid wenselijk zijn dit punt ook in de Wiv op te nemen.

Advies

De CTIVD adviseert in het voorgestelde artikel 126 een verwijzing naar het bepaalde in lid 5 van artikel 8:29 Awb en in artikel 8:31 Awb op te nemen.

Anna van Saksenlaan 50 | 2593 HT Den Haag
T 070 315 58 20 | **F** 070 381 71 68
E info@ctivd.nl | www.ctivd.nl