Toezichtsrapport

De multilaterale gegevensuitwisseling door de AIVD over (vermeende) jihadisten

CTIVD nr. 56

[vastgesteld op 7 februari 2018]

Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten

Commissie van Toezicht
op de Inlichtingen- en
Veiligheidsdiensten

CTIVD nr. 56

TOEZICHTSRAPPORT

De multilaterale gegevensuitwisseling door de AIVD over (vermeende) jihadisten

Inhoudsopgave

1 Inleiding 7

2 Algemeen beeld 11

3 Samenwerkingsverbanden en –vormen 12

3.1 Onderzochte samenwerkingsverbanden 12

3.2 Samenwerkingsvormen binnen de CTG 12

3.3 Samenwerkingsvormen binnen de sigint samenwerking 13

3.4 Overige samenwerkingsverbanden 13

4 Toetsingskader Wiv 2002 15

5 Grondslag voor samenwerking 17

5.1 Inleiding 17

5.2. Politiek-bestuurlijke context van internationale samenwerking 17

5.3. Nationale juridische grondslag voor samenwerking 19

5.4. Multilaterale afspraken m.b.t. samenwerkingsvormen 21

5.5 Toetsing van de grondslag voor de multilaterale gegevensuitwisseling 21
5.5.1 Risicoweging per buitenlandse dienst 21
5.5.2 Juridische grondslag database CTG 22
5.5.3 Juridische grondslag sigint samenwerking 27

6 Waarborgen 29

6.1 Inleiding 29

6.2 Waarborgen voor multilaterale gegevensuitwisseling 29

6.3 Waarborgen voor de gegevensuitwisseling door de AIVD binnen de CTG 30

6.4 Waarborgen voor de gegevensuitwisseling door de AIVD binnen de sigint samenwerking 31

8 Risico's en aanbevelingen 39

8.1 Inleiding 39

8.2 Risico's m.b.t. de CTG database 39
8.2.1 Risico's m.b.t. de juridische grondslag 39
8.2.2 Risico's voor noodzakelijkheid 40
8.2.3 Risico's voor behoorlijkheid 40
8.2.4 Risico's voor zorgvuldigheid 40
8.2.5 Risico's voor betrouwbaarheid 41

8.3 Risico's m.b.t. het operationeel platform van de CTG 42
8.3.1 Risico's voor zorgvuldigheid 42

8.4 Risico's m.b.t. samenwerkingsvormen binnen de sigint samenwerking 42
8.4.1 Risico's m.b.t. de grondslag voor een bepaalde samenwerkingsvorm 42
8.4.2 Risico's voor zorgvuldigheid 43

CTIVD nr. 56

SAMENVATTING

De multilaterale gegevensuitwisseling door de AIVD over (vermeende) jihadisten

De dreiging die uitgaat van het gewelddadig jihadisme is complex en diffuus. Terroristische aanslagen, zoals die in Brussel, Parijs en Londen worden voorbereid en uitgevoerd binnen terroristische organisaties, grensoverschrijdende netwerken, kleinschalige cellen of soms door eenlingen. Het op tijd onderkennen van de dreiging die hiervan uitgaat, en vervolgens het wegnemen daarvan, is geen eenvoudige opgave.

In Nederland is gekozen voor een integrale aanpak jihadismebestrijding waarbij de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) een belangrijke rol speelt. Internationaal is sprake van een zeer breed palet aan samenwerkingsinitiatieven tussen landen in Europa en daarbuiten. De multilaterale samenwerking met buitenlandse diensten is in dit kader essentieel om zicht te krijgen op de dreiging voor de (inter)nationale veiligheid. De AIVD vervult bij die samenwerking regelmatig een voortrekkersfunctie en onderhoudt op dit terrein intensieve en verregaande samenwerkingsrelaties met inlichtingen- en veiligheidsdiensten van andere landen.

De Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (CTIVD) heeft diepgaand onderzoek verricht naar de uitwisseling van persoonsgegevens m.b.t. (vermeende) jihadisten door de AIVD binnen de Counter-Terrorism Group (CTG) en in het kader van samenwerking op het gebied van *signals intelligence* (sigint). Het gaat bij de sigint samenwerking om het uitwisselen van gegevens afkomstig uit allerlei vormen van telecommunicatie. Hierbij is ook de Militaire Inlichtingen- en Veiligheidsdienst (MIVD) betrokken. Het onderzoek richt zich op de uitwisseling van persoonsgegevens vanaf begin 2015 tot medio 2017. Het betreft het eerste deel van een tweeluik. Het tweede deel gaat over de gegevensverstrekking m.b.t. (vermeende) jihadisten in de nationale context. Het rapport hierover verschijnt in het voorjaar van 2018.

Multilaterale gegevensuitwisseling over (vermeende) jihadisten vindt plaats met diensten binnen en buiten Europa en neemt verschillende vormen aan. De CTIVD signaleert daarbij een duidelijke ontwikkeling gericht op het sneller en effectiever delen van persoonsgegevens. Er wordt en is gezocht naar nieuwe manieren van (geautomatiseerde) gegevensuitwisseling en het fysiek dichter bij elkaar brengen van samenwerkingspartners, bijvoorbeeld in de recent opgerichte database en het zogenoemde operationeel platform van de CTG. De multilaterale samenwerking door de AIVD met inlichtingen- en veiligheidsdiensten van andere landen is in de afgelopen jaren sterk geïntensiveerd.

Tegen deze achtergrond heeft de CTIVD onderzoek verricht naar de juridische grondslag van bepaalde samenwerkingsvormen en bekeken hoe de multilaterale samenwerking als geheel is ingericht en functioneert. Daarbij heeft zij onderzocht in hoeverre het systeem van multilaterale gegevensuitwisseling voldoende waarborgen geeft voor de bescherming van het individu, gelet op het niveau van rechtsbescherming dat wordt geboden door onze Grondwet, het Europees Verdrag voor de Rechten van de Mens (EVRM) en in het bijzonder de Wiv 2002 (en de Wiv 2017). In aanvulling daarop

is onderzocht in hoeverre het interne beleid van de AIVD adequate waarborgen geeft. De CTIVD heeft dit getoetst aan de hand van de wettelijke vereisten voor noodzaak, zorgvuldigheid, behoorlijkheid en betrouwbaarheid voor de verwerking van persoonsgegevens. Deze vereisten blijven onder de nieuwe Wiv 2017 onverkort gelden. De CTIVD heeft steekproeven genomen van de toepassing daarvan in de praktijk.

De resultaten van dit onderzoek geven als het ware een foto van de huidige samenwerking. Het betreft een momentopname die inzichtelijk maakt waar op dit moment sprake is van voldoende waarborgen voor de rechtsbescherming van het individu, waar dit nog niet het geval is en daarmee mogelijk risico's m.b.t. die rechtsbescherming aan de orde zijn. Langs deze weg heeft de CTIVD in haar onderzoeksopzet, bevindingen, conclusies en aanbevelingen beoogd recht te doen aan de ontwikkeling waarin de multilaterale samenwerking zich bevindt.

De CTIVD constateert dat nu nog onvoldoende waarborgen bestaan voor de bescherming van het individu bij de uitwisseling en verdere verwerking van gegevens in het kader van de onderzochte multilaterale samenwerking. Het is voor een rechtmatige gegevensuitwisseling door de AIVD van belang dat deze situatie niet blijft voortbestaan en dat het niveau van rechtsbescherming wordt versterkt.

De CTIVD is van oordeel dat waar de multilaterale samenwerking door de AIVD met buitenlandse diensten leidt tot de gezamenlijke opslag en verwerking van persoonsgegevens of de gezamenlijke inzet van (bijzondere) bevoegdheden, sprake is van een *gezamenlijke verantwoordelijkheid*. Daarbij is elk van de deelnemende diensten aansprakelijk voor het geheel, dat wil zeggen voor de gevolgen van eventueel onrechtmatig handelen. Het is dan noodzakelijk dat de samenwerkende diensten met elkaar bepalen welke concrete *multilaterale* waarborgen zij *gezamenlijk* instellen voor de bescherming van de rechten van het individu. De algemene beginselen van gegevensbescherming zijn hiervoor leidend. De CTIVD constateert dat multilaterale waarborgen binnen de CTG slechts beperkt zijn ingevuld. In het kader van de sigint samenwerking is sprake van een hoger niveau van multilaterale gegevensbescherming.

De CTIVD heeft de gegevensuitwisseling door de AIVD getoetst aan de Wiv 2002 en de Wiv 2017. Zij is van oordeel dat de huidige uitvoeringspraktijk van deze gegevensuitwisseling op dit moment grotendeels nog binnen de kaders van de wettelijke vereisten blijft. Op twee punten is sprake van structurele onrechtmatigheid: het niet maken van een risicoweging aan de hand van de (wettelijke) criteria die gelden voor de samenwerking met buitenlandse diensten en het niet voorzien in een aanduiding van de betrouwbaarheid van door de AIVD verstrekte gegevens. Op één punt is sprake van een incidentele onrechtmatigheid: het gedurende vijf maanden ontbreken van toestemming van de minister van BZK (en van Defensie) voor de verstrekking van ongeëvalueerde gegevens bij de samenwerking op het gebied van sigint. Behoudens deze onrechtmatigheden, heeft de CTIVD geen door de AIVD multilateraal verstrekte persoonsgegevens aangetroffen die niet voldeden aan de vereisten van noodzakelijkheid, behoorlijkheid en zorgvuldigheid.

Vanwege de dreiging die uitgaat van het jihadisme en het grensoverschrijdende karakter van die dreiging, is het voor de AIVD noodzakelijk samen te werken met inlichtingen- en veiligheidsdiensten van andere landen. De CTIVD ziet echter risico's waar de waarborgen voor de bescherming van het individu nog onvoldoende zijn ingevuld. Een voorbeeld is het risico dat de samenwerkende diensten een steeds lagere drempel ervaren om persoonsgegevens uit te wisselen en de bescherming van grondrechten van burgers daarmee in het gedrang kan komen. Een ander risico ziet op het ontstaan van een groeiend gegevensbestand, waarvan het onvoldoende inzichtelijk is wat de juistheid en betrouwbaarheid is van de gegevens die daarin zijn opgenomen. Ook kan men denken aan het risico dat steeds meer persoonsgegevens mondeling worden uitgewisseld. Deze en andere risico's hebben zich in de praktijk nog niet of in zeer beperkte mate gemanifesteerd. Desondanks is het van wezenlijk

belang met deze risico's nu al rekening te houden, omdat deze in de nabije toekomst kunnen leiden tot onrechtmatig handelen van de AIVD in de multilaterale samenwerking met buitenlandse diensten. De CTIVD doet aanbevelingen die erop zijn gericht aanvullende waarborgen te stellen en daarmee onrechtmatig handelen voor te zijn. Hiermee beoogt de CTIVD een hoger beschermingsregime voor de burger te waarborgen en effectief toezicht mogelijk te maken.

In 2015 heeft de CTIVD het initiatief genomen tot een gezamenlijk project voor de afstemming van het toezicht op de multilaterale samenwerking bij de bestrijding van gewelddadig jihadisme. Samen met toezichthouders uit België, Denemarken, Noorwegen en Zwitserland worden onderzoeksmethoden vergeleken, juridische vraagstukken geduid en niet staatsgeheime bevindingen naast elkaar gelegd. Met het gezamenlijk project wordt beoogd de eerste stappen te zetten in het overbruggen van de grenzen van het nationaal toezicht. Genoemde toezichthouders streven ernaar begin 2018 te komen tot een gezamenlijk openbaar rapport.

CTIVD nr. 56

TOEZICHTSRAPPORT

De multilaterale gegevensuitwisseling door de AIVD over (vermeende) jihadisten

1 Inleiding

Aanleiding voor het onderzoek

De dreiging die uitgaat van het gewelddadig jihadisme is complex en diffuus. Niet alleen personen die zijn uitgereisd naar strijdgebieden in Syrië en Irak en daar vandaan terugkeren, vormen een dreiging voor Nederland. Dit geldt ook voor sympathisanten die in Nederland blijven. Het op tijd onderkennen van de dreiging die hiervan uitgaat, en vervolgens het wegnemen daarvan, is geen eenvoudige opgave.

In Nederland is gekozen voor een integrale aanpak jihadismebestrijding. Daartoe is in 2014 het Actieprogramma Integrale Aanpak Jihadisme opgezet op basis waarvan betrokken organisaties bijdragen aan het beschermen van de democratische rechtsstaat, het bestrijden en verzwakken van de jihadistische beweging in Nederland en het wegnemen van de voedingsbodem voor radicalisering. De Algemene Inlichtingen- en Veiligheidsdienst (AIVD) is een van de betrokken organisaties in het Actieprogramma en vormt een belangrijke schakel in dit geheel.

Internationaal is sprake van een zeer breed palet aan samenwerkingsinitiatieven. Zo wordt binnen de Verenigde Naties en de Europese Unie door lidstaten in allerlei gremia gezocht naar mogelijkheden gezamenlijk op te trekken in de strijd tegen het gewelddadig jihadisme. De samenwerking tussen inlichtingen- en veiligheidsdiensten vindt in het verlengde hiervan plaats, maar staat los van deze instituties. De AIVD onderhoudt op dit terrein intensieve samenwerkingsrelaties met inlichtingen- en veiligheidsdiensten van andere landen. Gegevensuitwisseling over (vermeende) jihadisten vindt plaats met buitenlandse diensten binnen en buiten Europa.

Context van het onderzoek

De CTIVD kondigde op 10 maart 2016 aan een onderzoek te zullen verrichten naar de gegevens-uitwisseling van de AIVD over (vermeende) jihadisten. Het onderzoek is gericht op gegevensuitwisseling vanaf 2015 in internationaal verband en gegevensverstrekking vanaf 2016 in nationaal verband. Het omvat twee fasen. Elke fase resulteert in ieder geval in een openbaar toezichtsrapport.

De eerste fase van het onderzoek richtte zich aanvankelijk op alle internationale gegevensuitwisseling van de AIVD over (vermeende) uitreizigers naar en terugkeerders uit het gebied Syrië/Irak. Na enige tijd onderzoek te hebben verricht, bracht de CTIVD een nadere focus aan. Zij besloot zich uitsluitend te richten op de multilaterale gegevensuitwisseling van de AIVD (tussen de AIVD en buitenlandse diensten in groepsverband). Dit eerste toezichtsrapport gaat dus over de gegevensuitwisseling van de AIVD binnen enkele multilaterale samenwerkingsverbanden. Deze samenwerking maakte de afgelopen

jaren een flinke ontwikkeling door. Bij de multilaterale samenwerking op het terrein van sigint is ook de Militaire Inlichtingen- en Veiligheidsdienst (MIVD) betrokken.

De tweede fase van het onderzoek is op 1 februari 2017 van start gegaan. Dat deel van het onderzoek gaat over gegevensverstrekking in nationaal verband. Door de AIVD verstrekte ambtsberichten aan onder meer het Openbaar Ministerie, de IND en burgemeesters, zijn bijvoorbeeld onderdeel van die fase. Het rapport hierover verschijnt in het voorjaar van 2018.

Scope van het onderzoek

De multilaterale samenwerking door de AIVD met buitenlandse diensten op het gebied van terrorismebestrijding is intensief en verregaand. Er is sprake van een hoge mate van vertrouwen in de buitenlandse diensten waarmee wordt samengewerkt. Er wordt onderling meer en meer openheid gegeven in het kennisniveau dat elke dienst heeft, in de gebruikte *modus operandi* (werkwijzen) en soms zelfs in de middelen of bronnen die zijn gebruikt om gegevens te verkrijgen.

De gegevensuitwisseling m.b.t. (vermeende) jihadisten die daarbij plaatsvindt, neemt verschillende vormen aan. In de onderzoeksperiode, vanaf begin 2015, is een duidelijke ontwikkeling gaande gericht op het sneller en effectiever delen van persoonsgegevens. Daarbij wordt en is gezocht naar nieuwe manieren van (geautomatiseerde) gegevensuitwisseling en het fysiek dichter bij elkaar brengen van samenwerkingspartners. Voorbeelden daarvan zijn de oprichting van een database en een operationeel platform in de Counter Terrorism Group (CTG), een Europees samenwerkingsverband tussen veiligheidsdiensten. Bij deze ontwikkelingen heeft de AIVD een belangrijke voortrekkersrol vervuld.

Hoewel het gaat om veelbelovende ontwikkelingen voor de internationale bestrijding van het gewelddadig jihadisme, brengen nieuwe vormen van samenwerking ook gevolgen met zich mee die juridisch moeten worden beoordeeld op rechtmatigheid.

Opzet van het onderzoek

De CTIVD signaleert dat gedurende haar onderzoek de ontwikkelingen binnen de multilaterale samenwerking een vlucht hebben genomen. De AIVD heeft daarbij veelal een pragmatische weg gekozen. Dit heeft mede geleid tot een relatief snelle intensivering van de multilaterale samenwerking tussen inlichtingen- en veiligheidsdiensten. De CTIVD heeft zich in haar onderzoek voortdurend de vraag gesteld waar, in deze steeds veranderende omstandigheden, de verantwoordelijkheden van de AIVD liggen resp. of deze op basis van de Wiv 2002 voldoende zijn ingevuld.

Tegen deze achtergrond heeft de CTIVD gekozen voor een brede, systeemmatige benadering van haar rechtmatigheidsonderzoek. Zij heeft bekeken hoe de multilaterale samenwerking als geheel is ingericht en functioneert. Daartoe heeft zij onderzocht in hoeverre het systeem van multilaterale gegevensuitwisseling, bezien vanuit het perspectief van onze Grondwet, het Europees Verdrag voor de Rechten van de Mens (EVRM) en in het bijzonder de Wiv 2002 (en de Wiv 2017) voldoende waarborgen geeft voor de bescherming van het individu. In aanvulling daarop is onderzocht in hoeverre het interne beleid van de AIVD dergelijke waarborgen geeft. Ook zijn steekproeven genomen van de uitwerking daarvan in de praktijk.

De resultaten van dit onderzoek geven als het ware een foto van de huidige samenwerking. Het betreft een momentopname die inzichtelijk maakt waar op dit moment sprake is van voldoende waarborgen voor de bescherming van het individu, waar dit nog niet het geval is en mogelijk risico's aan de orde zijn. Langs deze weg heeft de CTIVD in haar onderzoeksopzet, bevindingen, conclusies en aanbevelingen beoogd recht te doen aan de ontwikkeling waarin de multilaterale samenwerking zich bevindt.

Onderzoeksvragen

In dit onderzoek heeft de volgende vraag centraal gestaan:

> *Hoe is de multilaterale gegevensuitwisseling van de AIVD over (vermeende) jihadisten ingericht en is deze gegevensuitwisseling rechtmatig?*

Deze hoofdvraag valt uiteen in de volgende deelvragen:

1. *Welke rol vervult de AIVD in de multilaterale aanpak van het internationaal jihadisme? Binnen welke multilaterale samenwerkingsverbanden wisselt de AIVD persoonsgegevens uit in het kader van de aanpak van jihadisten?*
2. *Hoe worden persoonsgegevens uitgewisseld? Welke (nieuwe) samenwerkingsvormen vinden plaats?*
3. *Wat is de juridische grondslag voor de aangetroffen vormen van gegevensuitwisseling?*
4. *Is sprake van voldoende waarborgen voor de bescherming van grondrechten? Hoe geeft de AIVD in de praktijk invulling aan die waarborgen?*
5. *Is sprake van risico's die geadresseerd moeten worden?*

Leeswijzer

In hoofdstuk 2 geeft de CTIVD het algemene beeld dat het onderzoek haar heeft opgeleverd. In hoofdstuk 3 wordt een overzicht gegeven van de multilaterale samenwerkingsverbanden en samenwerkingsvormen die zijn onderzocht. Hoofdstuk 4 geeft een korte samenvatting van het juridisch kader dat van toepassing is op de samenwerking door de AIVD met buitenlandse diensten en de uitwisseling van persoonsgegevens in dat kader. Hoofdstuk 5 gaat in op de juridische grondslag en politieke context van de samenwerking en de samenwerkingsvormen die zich in dat kader aanzienlijk hebben ontwikkeld. In hoofdstuk 6 wordt ingegaan op de waarborgen voor de bescherming van grondrechten die bij deze samenwerkingsvormen aan de orde zijn en op welke wijze de AIVD invulling geeft aan deze waarborgen. De conclusies van de CTIVD zijn opgenomen in hoofdstuk 7. In hoofdstuk 8 bespreekt de CTIVD waar risico's aanwezig zijn of in de nabije toekomst voorzienbaar zijn en doet zij hiervoor aanbevelingen. Het rapport heeft verder vier bijlagen waarin de onderzoeksmethodiek (I), de bevindingen over waarborgen (II), gehanteerde begrippen (III) en een deskundigenbericht (IV) zijn opgenomen.

Van dit rapport is ook een geheime variant gemaakt. In het geheime toezichtsrapport zijn de hoofdstukken 3, 5, 6 en 8 en Bijlage II uitgebreider en gedetailleerder beschreven. De inleiding, het algemeen beeld, het juridisch kader, de conclusies en de Bijlagen I, III en IV zijn in beide rapporten echter volledig gelijkluidend.

Deskundigenbericht

De CTIVD heeft op basis van artikel 76 Wiv 2002 een deskundigenbericht doen opstellen over de juridische grondslag en verantwoordelijkheidsverdeling m.b.t. een specifieke samenwerkingsvorm. In paragraaf 5.5 wordt nader ingegaan op de inhoud van het deskundigenbericht. Het deskundigenbericht is bij het toezichtsrapport gevoegd als bijlage IV.

Samenwerking met andere toezichthouders

De CTIVD heeft in 2015 het initiatief genomen tot een gezamenlijk project, samen met toezichthouders uit België, Denemarken, Noorwegen en Zwitserland. Elk van deze toezichthouders verricht vanuit de eigen nationale context en binnen het eigen mandaat een onderzoek naar gegevensuitwisseling over (vermeende) jihadisten. Het project is erop gericht onderzoeksmethoden te vergelijken, juridische vraagstukken te duiden en niet staatsgeheime bevindingen naast elkaar te leggen.

Met het gezamenlijk project wordt beoogd de eerste stappen te zetten in het overbruggen van de grenzen van het nationaal toezicht, ook wel aangeduid als het *accountability deficit*. Door het naast

elkaar leggen van bevindingen en conclusies komt men tot een completer beeld van de internationale samenwerking tussen inlichtingen- en veiligheidsdiensten. Tegelijk maakt het inzichtelijker waar in dit verband bij de optelsom van ieders nationaal toezicht beperkingen aan de orde zijn. De deelnemers aan het project streven ernaar in 2018 te komen tot een gezamenlijk openbaar rapport.

2 Algemeen beeld

Het algemeen beeld van de CTIVD is dat de multilaterale samenwerking door de AIVD met buitenlandse diensten in het kader van jihadismebestrijding vergaande vormen aanneemt. De samenwerking heeft in de afgelopen jaren aan intensiteit gewonnen. Ook is gezocht naar andere, effectievere vormen van gegevensuitwisseling. De AIVD heeft hier een voortrekkersrol in gespeeld, met name tijdens het Nederlands voorzitterschap binnen de CTG in de eerste helft van 2016 en in de periode daarna.

De CTIVD signaleert dat het in het kader van brede multilaterale samenwerkingsverbanden waaraan een groot aantal diensten deelneemt, op zich niet eenvoudig is nieuwe initiatieven van de grond te krijgen en overeenstemming te bereiken over hoe de samenwerking ingericht moet zijn. Dergelijke processen vragen veel discussie en hebben een langere adem nodig. Desondanks hebben ontwikkelingen op dit terrein soms in korte tijd een vaart genomen. De AIVD zet zich hiervoor actief in en heeft in gezamenlijkheid met andere diensten een breed palet aan multilaterale afspraken weten te bereiken.

Het is niet eenvoudig daarbij direct een goede verhouding te vinden in wat soms tegenstrijdige belangen zijn. Enerzijds de operationele noodzaak en politieke wenselijkheid zo veel mogelijk relevante gegevens op zo kort mogelijke termijn uit te wisselen en anderzijds het belang de gegevensuitwisseling op een bestendige manier invulling te geven en juridisch verantwoord in te kaderen. De AIVD heeft daarin steeds een pragmatische weg gekozen en zich gericht op wat de dienst haalbaar leek op het gegeven moment.

Gedurende haar onderzoek heeft de CTIVD de ontwikkelingen op beide vlakken zien versnellen en stabiliseren. Met name de gevoelde operationele noodzaak tot meer en betere gegevensuitwisseling, bijvoorbeeld na aanslagen als in Brussel, Parijs en Londen, fungeert steeds als katalysator voor intensivering van samenwerkingsvormen. Daarop volgend komt doorgaans de bestendiging in afspraken of procedures, waar ook meer oog is voor de juridische kant van de gegevensuitwisseling. Deze ontwikkelingen lijken een bepaalde cadans te volgen en dienen op de langere termijn uiteindelijk min of meer gelijk op te gaan. Het is nu noodzakelijk dat de ontwikkelfase waarin de samenwerking zich bevindt, wordt gevolgd door een consolidatiefase waarin aandacht wordt besteed aan het instellen van aanvullende waarborgen voor de bescherming van het individu.

Hoewel de CTIVD dus ziet dat er veel gebeurt en hard wordt gewerkt, is zij kritisch. Bijvoorbeeld over het ontbreken van zogenoemde wegingsnotities en daarmee over het ontbreken van de formeel juridische grondslag van de multilaterale samenwerkingsrelaties van de AIVD. Kritisch ook over de juridische basis voor bepaalde samenwerkingsvormen en de verantwoordelijkheden die dit met zich mee brengt voor de AIVD en zijn samenwerkingspartners. De intensivering van de samenwerking is van die orde en grootte dat dit kan leiden tot de ontwikkeling van samenwerkingsvormen met potentieel verstrekkende gevolgen voor het individu, zonder dat daar voldoende bescherming van grondrechten en effectieve rechtsmiddelen tegenover komen te staan. Het is noodzakelijk dit voor te zijn, door tijdig adequate waarborgen in te stellen.

Adequate waarborgen dienen in de samenwerking in ieder geval ook multilateraal te worden ingevuld waar sprake is van de gezamenlijke opslag en verwerking van persoonsgegevens of de gezamenlijke inzet van (bijzondere) bevoegdheden. De vastlegging van gezamenlijke verantwoordelijkheden daarbij is essentieel. Daar waar waarborgen in de samenwerking ontbreken, niet vastgelegd of onvoldoende krachtig zijn, is sprake van risico's voor de bescherming van de grondrechten van de burger. Risico's die, wanneer deze zich verwezenlijken, ook kunnen leiden tot onrechtmatig handelen door de AIVD. De CTIVD signaleert deze risico's op een aantal terreinen (zie paragraaf 8).

3 Samenwerkingsverbanden en –vormen

3.1 Onderzochte samenwerkingsverbanden

De CTIVD heeft onderzoek verricht naar samenwerkingsverbanden waarbinnen multilateraal persoonsgegevens worden uitgewisseld. Het betreft onder meer de CTG, een samenwerkingsverband tussen de 30 veiligheidsdiensten van de EU-landen, Noorwegen en Zwitserland. De CTG is opgezet door de hoofden van een aantal Europese veiligheidsdiensten na de aanslagen in de Verenigde Staten op 11 september 2001. Ook werkt de AIVD multilateraal samen op het terrein van sigint. De sigint samenwerking is mede gericht op de bestrijding van terrorisme. De MIVD neemt eveneens hieraan deel. De verschillende samenwerkingsverbanden zijn opgericht op initiatief van de betrokken (gelijkgezinde) inlichtingen- of veiligheidsdiensten en zijn geen onderdeel van de EU, de VN of andere internationale dan wel supranationale organisaties.

Zowel in CTG verband als binnen de sigint samenwerking is sprake van het multilateraal delen van *geëvalueerde* gegevens over (vermeende) jihadisten. Met geëvalueerde gegevens wordt bedoeld gegevens die op hun waarde voor het inlichtingenproces zijn beoordeeld. Het betreft hier voornamelijk persoonsgegevens.

In het kader van de sigint samenwerking worden ook *ongeëvalueerde* gegevens in grote hoeveelheden (bulk) multilateraal uitgewisseld. Op het terrein van jihadismebestrijding gaat het vooralsnog om de uitwisseling van metadata van communicatie die een oorsprong of bestemming heeft in een bepaald gebied. Bijzonder aan de sigint samenwerking is verder dat gezamenlijke inlichtingenproducten worden gemaakt. Deze inlichtingenproducten zijn niet afkomstig van één van de deelnemende diensten, maar van de samenwerkende diensten als geheel.

De verschillende samenwerkingsverbanden werken niet direct samen. Er is wel sprake van indirecte verbindingen tussen de samenwerkingsverbanden.

De onderzochte multilaterale samenwerking uit zich in verschillende samenwerkingsvormen en gegevensstromen. In het geheime toezichtsrapport worden deze nader in kaart gebracht. In dit openbare toezichtsrapport is het slechts mogelijk een korte beschrijving te geven van enkele samenwerkingsvormen binnen CTG.

3.2 Samenwerkingsvormen binnen de CTG

De doelstelling van de CTG is het intensiveren van de samenwerking en de uitwisseling van informatie op het gebied van contraterrorisme tussen de veiligheidsdiensten van de deelnemende landen. Daarbij is een keuze gemaakt van een meer op zichzelf staande setting, buiten het EU systeem.[1] Het idee is dat de CTG hierdoor kan functioneren als zelfstandig forum op het niveau van diensthoofden en directeuren terrorismebestrijding en de samenwerking tussen de veiligheidsdiensten wordt vergemakkelijkt.

Europol, veiligheidsdiensten van de Verenigde Staten, het EU Inlichtingen Analyse Centrum (INTCEN) en de EU coördinator voor terrorismebestrijding hebben een vorm van 'waarnemerschap' bij de

[1] Door de regering is recent aangegeven dat de samenwerking in CTG verband plaatsvindt conform de lijn die is neergelegd in artikel 4.2 EU Handvest en artikel 73 VwEU, zie Antwoorden op Kamervragen gesteld door het lid Verhoeven, *Aanhangsel Handelingen II* 2017/18, nr. 202. Vermoedelijk wordt bedoeld artikel 4 lid 2 van het EU Verdrag, waarin is opgenomen dat de nationale veiligheid de uitsluitende verantwoordelijkheid blijft van elke lidstaat.

CTG. Dit houdt in dat zij geregeld kunnen aanzitten bij (strategische) overleggen van de CTG. Het gaat hierbij niet om operationele overleggen. Vanuit het CTG samenwerkingsverband worden geen persoonsgegevens aan deze derde partijen verstrekt. De CTIVD heeft geen nader onderzoek naar het 'waarnemerschap' verricht.

Het voorzitterschap van de CTG loopt gelijk met het voorzitterschap van de EU. Onder Nederlands voorzitterschap in de eerste helft van 2016 is de samenwerking binnen de CTG op het terrein van de aanpak van jihadisme aanmerkelijk geïntensiveerd. Binnen de CTG worden op verschillende wijzen en binnen verschillende gremia (persoons)gegevens uitgewisseld over (vermeende) jihadisten. De CTIVD beperkt zich hier tot het bespreken van gegevensuitwisseling via een database en binnen een operationeel platform.

CTG database

Sinds 2001 wisselen de diensten die deel uitmaken van de CTG (persoons)gegevens uit over uitreizigers naar en terugkeerders uit bepaalde conflictgebieden. Teneinde de multilaterale gegevensuitwisseling te bevorderen is een database gecreëerd. Deze database is op 1 juli 2016 geactiveerd en is (near) real-time beschikbaar voor alle dertig aan de CTG deelnemende diensten. Dit houdt in dat wanneer gegevens door één van de deelnemende diensten aan de database worden toegevoegd, deze gegevens (vrijwel) direct inzichtelijk zijn voor de andere deelnemende diensten. In de database zijn en worden (persoons)gegevens opgenomen over (vermeende) jihadisten. De database draait op een server op Nederlands grondgebied.

Operationeel platform

In 2016 zijn ook belangrijke stappen gezet voor de oprichting van een operationeel platform, dat in januari 2017 formeel is geopend. Het geeft de mogelijkheid om multilateraal meer in detail operationeel overleg te voeren, doordat vertegenwoordigers van de deelnemende diensten fysiek bij elkaar zitten. Het operationeel platform is toegankelijk voor alle 30 CTG-diensten. Tijdens de bijeenkomsten van het platform worden zogenoemde plots besproken; dat wil zeggen concrete, vrij afgebakende casussen die zich lenen voor multilaterale operationele bespreking. Er vindt in het kader van het operationeel platform geen gezamenlijke inzet van bijzondere bevoegdheden plaats. Ook het operationeel platform bevindt zich op Nederlands grondgebied.

3.3 Samenwerkingsvormen binnen de sigint samenwerking

In het geheime toezichtsrapport worden de samenwerkingsvormen binnen de sigint samenwerking nader besproken.

3.4 Overige samenwerkingsverbanden

De AIVD participeert nog in een aantal andere multilaterale samenwerkingsverbanden waarbinnen direct of indirect wordt bijgedragen aan de internationale bestrijding van het jihadisme. Het gaat hierbij om technische of analytische samenwerking of om samenwerking in een zeer kleine groep. De CTIVD heeft ervoor gekozen niet alle samenwerkingsverbanden nader, dat wil zeggen diepgaand, te onderzoeken, ofwel omdat het zwaartepunt hierbij niet ligt bij het *multilateraal* uitwisselen van gegevens, ofwel omdat beperkt sprake is van het uitwisselen van persoonsgegevens.

In deze context is het nog van belang te vermelden dat er een multilateraal samenwerkingsverband is op het terrein van jihadistisch internet. Dit samenwerkingsverband is in 2007 opgericht om gezamenlijk de terrorismedreiging en de daaraan gerelateerde (technische) ontwikkelingen op het internet het hoofd te kunnen bieden. Gegevensuitwisseling vindt binnen dit samenwerkingsverband onder meer plaats

tijdens jaarlijkse bijeenkomsten. Bij deze bijeenkomsten worden operationele ervaringen, analyses en technologische ontwikkelingen besproken. Het gaat hier niet of nauwelijks om het uitwisselen van *persoonsgegevens* over vermeende jihadisten. Daarom wordt dit samenwerkingsverband niet nader besproken in dit toezichtsrapport.

Daarnaast is tussen de diensten die deelnemen aan dit verband sprake van het bilateraal delen van ongeëvalueerde gegevens, zoals webfora. Dit betreft wel persoonsgegevens. Er is echter geen sprake van *multilaterale* gegevensuitwisseling.[2]

[2] De CTIVD heeft de uitwisseling van webfora ook beoordeeld in de toezichtsrapporten nrs. 39 (onderzoek van de AIVD op sociale media) en 49 (uitwisseling van ongeëvalueerde gegevens).

4 Toetsingskader Wiv 2002

De CTIVD heeft het geldende toetsingskader voor het handelen van de AIVD in de samenwerking met buitenlandse diensten uiteengezet in eerdere toezichtsrapporten. Zij vindt het niet nodig het toetsingskader hier opnieuw integraal op te nemen.[3] In het kort geldt dat de AIVD bij de uitwisseling van persoonsgegevens, op basis van zowel de huidige als de nieuwe wet, de volgende overwegingen moet maken.

1. Komt een buitenlandse dienst in aanmerking voor samenwerking, op basis van een weging van risico's die in de samenwerking aan de orde kunnen zijn?

De AIVD mag samenwerken met buitenlandse diensten die daarvoor in aanmerking komen. Of een buitenlandse dienst in aanmerking komt voor samenwerking moet worden bepaald door het maken van een risicoafweging. De AIVD moet in kaart brengen van welke risico's in de samenwerking sprake kan zijn en onder welke omstandigheden die risico's aanvaardbaar zijn.

Deze weging dient te worden vastgelegd in een zogenoemde wegingsnotitie. Bij de weging moet worden betrokken in welke mate de buitenlandse dienst voldoet aan bepaalde samenwerkingscriteria, zoals respect voor mensenrechten, democratische inbedding en professionaliteit en betrouwbaarheid. De uitkomst van de weging bepaalt hoe ver de samenwerking mag gaan en welke grenzen daarvoor gelden.[4] De wegingsnotitie moet worden goedgekeurd door de minister van BZK. De Wiv 2017 voorziet in de mogelijkheid dit te mandateren aan het hoofd van de dienst.

Wanneer de AIVD vervolgens in een concrete situatie gegevens verstrekt aan een buitenlandse dienst of gegevens ontvangt en deze wil gebruiken, moet de dienst nog twee afwegingen maken:

2. Vindt de gegevensuitwisseling met de buitenlandse dienst plaats binnen de grenzen die zijn neergelegd in de wegingsnotitie?

Is dit niet het geval, dan moet daar iets tegenover staan. De AIVD moet beargumenteerd schriftelijk vastleggen dat sprake is van zwaarwegende operationele belangen die rechtvaardigen dat de dienst buiten de gestelde grenzen van de samenwerking treedt. Ook moet op een hoger niveau dan voor de gegevensuitwisseling gebruikelijk is, toestemming hiervoor worden verkregen. Bij de verstrekking van persoonsgegevens is in zo'n geval toestemming van de minister nodig.[5]

3. Voldoet de gegevensuitwisseling aan de eisen van noodzakelijkheid, behoorlijkheid, zorgvuldigheid en (aanduiding van) betrouwbaarheid die de Wiv 2002 stelt?[6]

---

[3] Het toetsingskader voor de samenwerking en gegevensuitwisseling met buitenlandse diensten is onder meer aan de orde geweest in de CTIVD rapporten nrs. 22a, 22b, 38, 48, 49 en 50. In rapport nr. 50 over bijdragen van de MIVD aan targeting is bovendien een schematische weergave van het toetsingskader opgenomen in paragraaf 3.1. Alle rapporten zijn beschikbaar op www.ctivd.nl.

[4] Zie voor een uitgebreide uiteenzetting CTIVD rapport nr. 48 over de invulling van samenwerkingscriteria door de AIVD en de MIVD, *Kamerstukken II* 2015/16, 29 924 nr. 142 (bijlage), ook beschikbaar op www.ctivd.nl.

[5] Kamerstukken II 2015/16, 29 924 nr. 142.

[6] Zie voor een bespreking van deze vereisten de juridische bijlage bij rapport nr. 22b over de samenwerking van de MIVD met buitenlandse diensten, *Kamerstukken II* 2014/15, 29 924 nr. 128 (bijlage) en de juridische bijlage bij rapport nr. 38 inzake de gegevensverwerking op het gebied van telecommunicatie door de AIVD en de MIVD, *Kamerstukken II* 2013/14, 29 924 nr. 105 (bijlage), ook beschikbaar op www.ctivd.nl.

Het gaat hier om eisen die zowel over de inhoud als over de vorm van de gegevensuitwisseling gaan. Zo moet de gegevensuitwisseling noodzakelijk zijn voor een vooraf vastgesteld doel, geen disproportioneel nadeel opleveren, worden onderbouwd door onderliggende gegevens en zijn voorzien van een bronvermelding of een aanduiding van betrouwbaarheid. De verstrekking van persoonsgegevens moet in beginsel schriftelijk plaatsvinden. Een nadere uitwerking van wat deze vereisten inhouden in het kader van multilaterale samenwerking, is opgenomen in bijlage II bij dit toezichtsrapport. De Wiv 2017 brengt geen verandering hierin.

In bepaalde gevallen zijn de afwegingen onder 3 niet goed te maken, onder meer bij de uitwisseling van ongeëvalueerde gegevens aan een buitenlandse dienst. Ongeëvalueerde gegevens zijn (veelal grotere hoeveelheden) gegevens die niet zijn beoordeeld op relevantie voor de taakuitvoering van de AIVD. Het is bij ongeëvalueerde gegevens op voorhand niet geheel duidelijk wat precies wordt verstrekt of ontvangen. Het is dan ook niet goed mogelijk de in de wet opgenomen noodzakelijkheid en behoorlijkheid van de gegevensuitwisseling voldoende af te wegen. Deze vereisten kunnen bij de uitwisseling van ongeëvalueerde gegevens slechts in algemene zin worden onderbouwd.

Voor dergelijke situaties is een aanvullende waarborg gecreëerd. In een motie van de Tweede Kamer die is aangenomen in april 2014, is de regering verzocht dergelijke gegevens pas uit te wisselen nadat toestemming is verkregen van de betrokken minister. De regering zegde dit toe.[7] De minister toetst niet alleen of de beoordeling die is neergelegd in de wegingsnotitie terecht is (onder 1). Hij moet ook beoordelen of de uitwisseling van ongeëvalueerde gegevens past binnen de grenzen die zijn aangegeven in de wegingsnotitie (onder 2) en, voor zover mogelijk, of de gegevensuitwisseling in het specifieke geval geoorloofd is (onder 3). Op deze manier maakt de minister de (politieke) afweging of de risico's die gepaard gaan met het uitwisselen van ongeëvalueerde gegevens aanvaardbaar zijn. Het is dan wel van wezenlijk belang dat er een wegingsnotitie is met betrekking tot de desbetreffende buitenlandse dienst.

[7] Zie voor een uitgebreide uiteenzetting CTIVD rapport nr. 49 over de uitwisseling van ongeëvalueerde gegevens door de AIVD en de MIVD, *Kamerstukken II* 2015/16, 29 924 nr. 142 (bijlage), ook beschikbaar op www.ctivd.nl.

5 Grondslag voor samenwerking

5.1 Inleiding

De in hoofdstuk 4 genoemde multilaterale samenwerking is intensief en verregaand. De gegevensuitwisseling over (vermeende) jihadisten die daarbij plaatsvindt, neemt allerhande vormen aan. Er is daarbij een duidelijke ontwikkeling gaande gericht op het sneller en effectiever delen van (persoons) gegevens. Daarbij wordt en is gezocht naar nieuwe manieren van gegevensuitwisseling en het fysiek dichter bij elkaar brengen van samenwerkingspartners.

De CTIVD heeft zich afgevraagd wat de grondslag is voor de gegevensuitwisseling van de AIVD binnen de desbetreffende multilaterale samenwerking en of deze grondslag bij de genoemde vormen van gegevensuitwisseling voldoet.

Een internationale, publiekrechtelijke grondslag voor de samenwerking is niet aan de orde. De samenwerking vindt buiten de EU, de VN of andere internationale dan wel supranationale organisaties plaats en is niet geregeld in formele, juridisch bindende afspraken, zoals een verdrag. De basis voor de gegevensuitwisseling door de AIVD dient dan ook in ieder geval gelegen te zijn in nationale wet- en regelgeving. Het internationaal recht, onder meer op het gebied van staatsaansprakelijkheid en op het gebied van gegevensbescherming, is desalniettemin relevant. Waar het gaat om de samenwerking tussen inlichtingen- en veiligheidsdiensten, zijn deze rechtsgebieden nog volop in ontwikkeling. Tegen deze achtergrond heeft de CTIVD opdracht gegeven aan twee deskundigen op voornoemde rechtsterreinen, een deskundigenbericht op te stellen m.b.t. de juridische grondslag en verantwoordelijkheidsverdeling van de CTG database (zie bijlage IV).

De CTIVD gaat in dit hoofdstuk eerst in op de politiek-bestuurlijke context van jihadismebestrijding, omdat deze van betekenis kan zijn voor de juridische grondslag van de samenwerking door de AIVD. Dit kan niet volledig los van elkaar worden gezien. Vervolgens gaat de CTIVD in op de juridische basis voor samenwerking met buitenlandse diensten die is neergelegd in de Wiv 2002 (en in de Wiv 2017). De Wiv 2002 geeft naast een algemene grondslag voor samenwerking specifiek de bevoegdheid gegevens te verstrekken en ondersteuning te verlenen aan buitenlandse diensten. In de Wiv 2017 is dit eveneens het geval. Voorts bespreekt de CTIVD multilaterale afspraken die een nadere invulling kunnen geven aan specifieke vormen van gegevensuitwisseling.

Elk van deze onderwerpen komt vervolgens terug in de laatste paragraaf van dit hoofdstuk, waarin de multilaterale gegevensuitwisseling op zijn grondslag wordt getoetst. De inhoud van het deskundigenbericht (zie bijlage IV) wordt nadrukkelijk in de toetsing betrokken.

5.2. Politiek-bestuurlijke context van internationale samenwerking

Nationaal beleid

De Nederlandse overheid zet met het Actieprogramma Integrale Aanpak Jihadisme[8] in op een brede aanpak van de jihadistische dreiging in Nederland. Deze aanpak verloopt langs vijf beleidslijnen, waaronder Informatie-uitwisseling en (internationale) samenwerking. Mede om gevolg te geven aan het Actieprogramma zet Nederland zich internationaal actief in. Nederland participeert actief in verschillende politiek-bestuurlijke internationale gremia die zich bezighouden met het tegengaan van

[8] *Kamerstukken II* 2013/14, 29 754 nr. 253 (bijlage).

de dreiging die voortkomt uit het gewelddadig jihadisme. Hoewel de AIVD niet rechtstreeks deelneemt hieraan, vormen de internationale samenwerkingsverbanden en strategieën waaraan Nederland zich politiek heeft gecommitteerd wel de achtergrond waartegen de AIVD zich beweegt. In elk van deze gremia (zie hieronder) wordt de noodzaak tot intensieve gegevensuitwisseling tussen staten benadrukt.

Verenigde Naties

In Resolutie 2178 (2014) van de VN Veiligheidsraad[9] worden lidstaten opgeroepen (strafrechtelijke) maatregelen te nemen tegen de dreiging die uitgaat van *foreign terrorist fighters*. Te nemen maatregelen dienen onder meer gericht te zijn op het voorkomen dan wel tegengaan van het rekruteren, organiseren, transporteren faciliteren van personen die uitreizen ten behoeve van de gewelddadige jihad. De VN lidstaten worden daarbij opgeroepen de (operationele) gegevensuitwisseling over *foreign terrorist fighters* te intensiveren en te versnellen. Ook wordt een definitie gegeven van *foreign terrorist fighter*. Nederland is gehouden uitvoering te geven aan Resolutie 2178 (2014). De implementatie van Resolutie 2178 krijgt o.a. vorm binnen het *Global Counter Terrorism Forum* (GCTF) en de anti-ISIS-coalitie.

Global Counter Terrorism Forum (GCTF)

Het GCTF is een internationaal forum van 29 landen en de EU.[10] Het forum biedt de mogelijkheid kennis en ervaringen te delen en middelen en strategieën te ontwikkelen in de bestrijding van het terrorisme. Nederland heeft vanaf september 2015 samen met Marokko het voorzitterschap van het GCTF. Ook heeft Nederland een leidende rol in de *Foreign Terrorist Fighters* werkgroep van het GCTF. Vanuit GCTF worden aanbevelingen gedaan voor het maken van beleid c.q. het nemen van nationale maatregelen m.b.t. jihadstrijders. De internationale uitwisseling van gegevens wordt daarbij gezien als een voorwaarde voor effectieve terrorismebestrijding.

Anti-ISIS-coalitie

Nederland neemt sinds oktober 2014 deel aan de anti-ISIS-coalitie, die in de strijd tegen ISIS onder meer luchtaanvallen uitvoert in Syrië en Irak. In deze coalitie zijn inmiddels meer dan 70 landen vertegenwoordigd. Nederland draagt zowel militair als diplomatiek bij aan de coalitie.[11] Nederland is verder drie jaar actief geweest als co-voorzitter, samen met Turkije, van de *Foreign Terrorist Fighter* werkgroep. In deze werkgroep wordt met name aandacht besteed aan de informatie-uitwisseling tussen internationale organisaties, zoals Interpol, en overheden, samenwerking met landen in de regio en de geïntegreerde aanpak van terugkeerders.[12]

Europese Unie

Binnen de EU is Nederland actief in de EU-kopgroep jihadgangers, in het kader waarvan nadere afstemming over de nationale aanpak van jihadstrijders plaatsvindt.[13] Kern van het actieplan van deze kopgroep is het Europees delen van informatie over uitreizigers. Maatregelen zijn gericht op grenstoezicht, informatie-uitwisseling en optimalisering van signaleringmogelijkheden van uitreizigers en terugkeerders, onder andere door beter gebruik te maken van bestaande instrumenten zoals het Schengen Informatie Systeem (SIS).[14]

---

9 S/RES/2178 (2014), 24 September 2014, onder 3.

10 Het GTCF is opgericht door: Algerije, Australië, Canada, China, Columbia, Denemarken, Duitsland, Egypte, de EU, Frankrijk, India, Indonesië, Italië, Japan, Jordanië, Marokko, Nederland, Nieuw Zeeland, Nigeria, Pakistan, Qatar, Rusland, Saoedi Arabië, Spanje, Turkije, de VAE, het VK, de VS, Zuid Afrika en Zwitserland; zie ook www.thegtcf.org.

11 *Kamerstukken II* 2016/17, 27 925 nr. 607.

12 *Kamerstukken II* 2016/17, 27 925 nr. 607.

13 De kopgroep bestaat uit Nederland, België, Frankrijk, Zweden, Denemarken, Italië, Spanje, het Verenigd Koninkrijk, Duitsland en Ierland.

14 Aanbiedingsbrief Tweede Voortgangsrapportage Actieprogramma, *Kamerstukken II* 2014-25, 29 754, nr. 308.

Onder Nederlands EU-voorzitterschap zijn de lidstaten in de JBZ Raad op 10 juni 2016 akkoord gegaan met de Routekaart voor het verbeteren van informatie-uitwisseling en informatiebeheer op het gebied van justitie en binnenlandse zaken.[15] Het gaat daarbij om rechtshandhaving, terrorismebestrijding en grensmanagement. De lidstaten hebben zich gecommitteerd tot de volgende afspraken: 1) alle relevantie informatie wordt gedeeld, tenzij er zwaarwegende juridische of operationele redenen zijn om dat niet te doen; 2) er wordt gewerkt op basis van vastgestelde principes, zoals het respecteren van grondrechten en regels voor gegevensbescherming; en 3) de samenwerking, kwaliteit en bruikbaarheid van systemen worden verbeterd. Tijdens dezelfde bijeenkomst is besloten dat de CTG voortaan aan de JBZ Raad kan deelnemen als terrorisme op de agenda staat. Hiermee wordt beoogt de samenwerking tussen de CTG en EU instanties die zich bezighouden met terrorismebestrijding te stimuleren.[16]

EU-beleid en -wetgeving vormen geen directe grondslag voor de activiteiten van de AIVD. De nationale veiligheid valt op grond van artikel 4 van het EU Verdrag buiten het bereik van de EU. Artikel 73 van het Verdrag betreffende de werking van de EU bepaalt bovendien dat het de lidstaten vrij staat onderling en onder hun verantwoordelijkheid vormen van samenwerking en coördinatie te organiseren tussen overheidsdiensten op het terrein van de nationale veiligheid.

5.3. Nationale juridische grondslag voor samenwerking

De Wiv 2002 geeft niet voor elke samenwerkingsvorm een expliciete juridische grondslag. De wet stelt dat voorafgaande aan de samenwerking met buitenlandse diensten een afweging dient plaats te vinden of de desbetreffende buitenlandse dienst in aanmerking komt voor de samenwerking. Daarnaast geeft de Wiv 2002 een expliciete grondslag voor het verstrekken van gegevens en voor het verlenen van ondersteuning.

Risicoweging

Op basis van de Wiv 2002 draagt het hoofd van de AIVD zorg voor de samenwerking met daarvoor in aanmerking komende buitenlandse inlichtingen- en veiligheidsdiensten (artikel 59 lid 1). Of buitenlandse diensten voor samenwerking in aanmerking komen, moet worden bepaald aan de hand van een risicoweging. De weging bepaalt hoe ver de samenwerking met een buitenlandse dienst kan gaan en welke vormen van samenwerking daarbij geoorloofd zijn. Het is vervolgens een politieke afweging of de geïdentificeerde risico's in de samenwerkingsrelatie met de desbetreffende dienst aanvaardbaar worden geacht. De rechtmatigheidsbeoordeling blijft evenwel een juridische afweging.

De mate waarin een buitenlandse dienst voldoet aan bepaalde samenwerkingscriteria moet bij de weging worden betrokken. Het gaat hier onder meer om samenwerkingscriteria als respect voor mensenrechten, professionaliteit en het geboden niveau voor gegevensbescherming die zich specifiek richten op de buitenlandse dienst. Ook zijn er criteria voor de samenwerking zelf, zoals de mate waarin de samenwerking ten dienste staat aan de taakuitvoering van de AIVD of de wenselijkheid in het kader van internationale verplichtingen. Bij dit laatste moet worden beoordeeld of de samenwerking wenselijk of onwenselijk is in het licht van het Nederlands buitenlandbeleid en verplichtingen die voortvloeien uit het lidmaatschap van internationale organisaties, zoals de Verenigde Naties.

De samenwerkingscriteria vloeien voort uit de wetsgeschiedenis en uit aanbevelingen van de CTIVD in eerdere toezichtsrapporten die zijn overgenomen door de betrokken ministers. In de nieuwe Wiv 2017 is de weging aan de hand van deze samenwerkingscriteria expliciet wettelijk geregeld. In een overgangsbepaling (artikel 166 Wiv 2017) wordt de invoering van deze systematiek, die onder

[15] 9368/1/16 REV1.

[16] *Kamerstukken II* 2015/16, 27 925 nr. 595.

de huidige wet ook al geldt, met twee jaar uitgesteld voor bestaande samenwerkingsrelaties. Dit heeft tot gevolg dat de AIVD (en de MIVD) formeel voorlopig niet verplicht is aan de hand van de samenwerkingscriteria te bepalen of met een buitenlandse dienst kan worden samengewerkt en welke vormen van samenwerking daarbij geoorloofd zijn op basis van de geconstateerde risico's.

In een brief van 15 december 2017[17] hebben de ministers van BZK en Defensie toegezegd dat bij de inwerkingtreding van de Wiv 2017 de wegingsnotities m.b.t. de meest hechte samenwerkingsrelaties van de AIVD (en de MIVD) reeds vastgesteld zullen zijn. Hieronder worden begrepen de buitenlandse diensten die deelnemen aan de CTG en diensten waarmee op het terrein van sigint intensief wordt samengewerkt.

Gegevensverstrekking

In de Wiv 2002 (en de Wiv 2017) zijn bepalingen opgenomen over de verstrekking van gegevens. Artikel 36 geeft de AIVD de bevoegdheid gegevens te verstrekken aan daarvoor in aanmerking komende buitenlandse diensten in het kader van de eigen taakuitvoering. Ook is het toegestaan gegevens te verstrekken in het belang van de buitenlandse dienst (artikel 59 lid 2). Het kan hier zowel om geëvalueerde als ongeëvalueerde gegevens gaan. Deze wetsartikelen vormen de basis voor elke verstrekking van gegevens door de AIVD aan buitenlandse diensten.

Voor het ontvangen en gebruiken van gegevens van buitenlandse diensten is geen specifieke bepaling in de wet opgenomen. De grondslag hiervoor ligt besloten in de bevoegdheid om te mogen samenwerken (artikel 59 lid 1). Verder geldt dat voor de verwerking van ontvangen gegevens doorgaans dezelfde interne procedures gelden als voor gegevens die eigenstandig door de AIVD verworven zijn. Het gebruik van die gegevens moet bovendien voldoen aan de algemene vereisten voor gegevensverwerking (zie ook het toetsingskader in hoofdstuk 3).

De wijze waarop gegevens worden uitgewisseld, staat grotendeels vrij. De wet geeft voorschriften voor de wijze waarop gegevens moeten worden verstrekt. Aan de verstrekking moet de voorwaarde worden gesteld dat de ontvangende partij de gegevens niet aan anderen mag verstrekken (artikel 37).[18] De verstrekking van persoonsgegevens moet in beginsel schriftelijk gebeuren (artikel 40). Voor de vorm waarin gegevens worden uitgewisseld, geeft de Wiv 2002 (en de Wiv 2017) geen verdere beperkingen aan.

Ondersteuning

De Wiv 2002 (en de Wiv 2017) geeft ook een grondslag voor het verlenen van ondersteuning in het belang van een buitenlandse dienst. Bij het verlenen van ondersteuning kan het gaan om de inzet van bijzondere bevoegdheden. Een schriftelijk verzoek van de desbetreffende buitenlandse dienst en voorafgaande toestemming van de betrokken minister zijn vereist.

In de Wiv 2017 is in aanvulling op deze regeling ook geregeld dat de AIVD (of MIVD) zelf een verzoek om ondersteuning doet aan een buitenlandse dienst (artikel 90). Hieraan wordt onder meer de voorwaarde gesteld dat het verzoek geen betrekking kan hebben op het verrichten van handelingen die niet overeenkomen met de uitoefening van een bevoegdheid als bedoeld in de Wiv 2017.

---

17 *Kamerstukken II*, 2017/18, 34588 nr. 69.

18 In rapport nr. 50 over bijdragen van de MIVD aan targeting heeft de CTIVD aanbevolen dat onder bepaalde omstandigheden ook de voorwaarde moet worden gesteld dat gegevens niet mogen worden gebruikt voor doeleinden die een schending van het internationaal recht inhouden (hoofdstuk 6, aanbeveling 5), beschikbaar op www.ctivd.nl. Deze aanbeveling is door de minister van Defensie overgenomen. Het hoofd van de AIVD heeft op 19 mei 2017 aan de CTIVD kenbaar gemaakt deze voorwaarde eveneens onder bepaalde omstandigheden te stellen.

5.4. Multilaterale afspraken m.b.t. samenwerkingsvormen

Multilaterale afspraken tussen inlichtingen- en veiligheidsdiensten kunnen een nadere invulling geven aan specifieke vormen van samenwerking. Binnen de onderzochte multilaterale samenwerking is sprake van afspraken waaraan elke partij zich committeert, maar die juridisch niet bindend zijn en niet kunnen worden afgedwongen.

Binnen de CTG zijn multilaterale afspraken vastgesteld. Zo is beschreven wat de doelstelling is van de samenwerking binnen de CTG, hoe de CTG georganiseerd is en op welke wijze beslissingen worden genomen. Ook zijn afspraken opgenomen over lidmaatschap, geheimhouding en de verstrekking van gegevens aan derden. Met betrekking tot de database en het operationeel platform zijn procedures en werkafspraken vastgelegd. Zo is vastgelegd waar de database c.q. het platform voor bedoeld zijn, wie waarvoor verantwoordelijk is, op welke wijze het gebruikt kan worden en hoe het zich verhoudt tot andere instrumenten in de bestrijding van het jihadisme, zoals nationale en internationale grens signaleringssystemen.

Binnen de sigint samenwerking is ervoor gekozen afspraken over specifieke samenwerkingsvormen neer te leggen in een document dat door de ministers van BZK en Defensie is ondertekend. Deze multilaterale afspraken hebben daarmee een iets zwaarder karakter, maar blijven desondanks niet juridisch afdwingbaar. De afspraken geven invulling aan de wijze waarop hier concreet wordt samengewerkt. Ook wordt in dit kader aandacht besteed aan het toezicht hierop door nationale toezichthouders.

Multilateraal gemaakte afspraken hebben slechts gelding voor zover nationale wet- en regelgeving daarvoor de ruimte biedt. De CTIVD beschouwt dergelijke documenten als het internationale equivalent van intern beleid. De AIVD heeft zich gecommitteerd aan de multilaterale afspraken die daarin zijn opgenomen. Daarmee maakt het deel uit van het regelgevend kader waaraan de AIVD zich heeft te houden. Net als bij intern beleid van de AIVD kan het toezicht zich richten op de vraag of het beleid in overeenstemming is met de Wiv 2002 (en straks de Wiv 2017) en of het beleid in de praktijk door de AIVD wordt nageleefd.

Het voorgaande neemt niet weg dat multilaterale afspraken essentieel zijn in het voldoen aan nationale wet- en regelgeving en bijdragen aan de bescherming van de grondrechten van de burger.[19] In hoofdstuk 6 wordt dan ook nader ingegaan op de wijze waarop de AIVD invulling geeft aan waarborgen die voortvloeien uit multilaterale afspraken. De risico's die daarbij kunnen bestaan, worden in hoofdstuk 8 geadresseerd, gelet op de bescherming van grondrechten die de Wiv 2002 (respectievelijk de Wiv 2017) beoogt te bieden.

5.5 Toetsing van de grondslag voor de multilaterale gegevensuitwisseling

5.5.1 Risicoweging per buitenlandse dienst

Aan de vereiste beoordeling of een buitenlandse dienst voor samenwerking in aanmerking komt, wordt door de AIVD niet voldaan.[20] Er zijn vooralsnog geen wegingsnotities vastgesteld m.b.t. de buitenlandse diensten waarmee de AIVD samenwerkt in multilateraal verband. Dit leidt ertoe dat de legitimiteit van de samenwerkingsrelatie van de AIVD met elk van de buitenlandse diensten onvoldoende geborgd is.

---

[19] Zie ook het deskundigenbericht in bijlage IV bij dit toezichtsrapport.

[20] CTIVD rapport nr. 48 over de invulling van samenwerkingscriteria door de AIVD en de MIVD, *Kamerstukken II* 2015/16, 29 924 nr. 142 (bijlage), ook beschikbaar op www.ctivd.nl.

De weging heeft immers een constituerende functie voor samenwerking. Het is de basis waarop de AIVD de samenwerkingsrelatie dient te berusten. Het bepaalt de bandbreedte waarbinnen de AIVD zich in de samenwerking verantwoord kan bewegen. Het treden buiten die bandbreedte is in beginsel te risicovol en slechts geoorloofd indien daar zwaarwegende operationele belangen tegenover staan. De CTIVD heeft vanaf 2009 in verschillende toezichtsrapporten het belang hiervan benadrukt en aanbevolen per buitenlandse dienst gedegen wegingsnotities op te stellen. Zonder weging mist de samenwerking zijn formele grondslag.

Voor de CTIVD roept het de vraag op wat dit betekent voor de rechtmatigheid van de onderzochte gegevensuitwisseling over (vermeende) jihadisten van de AIVD binnen de CTG en de multilaterale samenwerking op het terrein van sigint. Komen de desbetreffende buitenlandse diensten inderdaad *in aanmerking* voor deze specifieke vormen van samenwerking? Waar het gaat om gegevensuitwisseling ter bestrijding van het gewelddadig jihadisme is dat echter al snel een gegeven. Gelet op het zwaarwegende belang hiervan, dat nationaal en internationaal breed gedeeld wordt, en gelet op de internationale verplichtingen die Nederland in dat kader is aangegaan, is het niet reëel te stellen dat de desbetreffende buitenlandse diensten daarvoor niet in aanmerking zouden komen. De noodzaak van de gezamenlijke bestrijding van het gewelddadig jihadisme weegt immers al snel op tegen eventuele risico's die in de multilaterale samenwerking aan de orde kunnen zijn.[21]

Dit neemt niet weg dat het desondanks van groot belang is dat de AIVD inzichtelijk maakt of sprake is van risico's voor de gegevensuitwisseling met de buitenlandse diensten waarmee wordt samengewerkt, en zo ja, welke risico's dat zijn. Ook in het kader van terrorismebestrijding dient de AIVD zich hier rekenschap van te geven. Een risicoweging neergelegd in een wegingsnotitie zal er naar alle waarschijnlijkheid niet toe leiden dat de samenwerking met de desbetreffende buitenlandse diensten op het terrein van jihadismebestrijding wordt beperkt of dat de gegevensuitwisseling wordt teruggebracht. Het dwingt er echter wel toe dat de AIVD aanvullende waarborgen instelt waar risico's aan de orde zijn respectievelijk zich in de toekomst zullen manifesteren.

5.5.2 Juridische grondslag database CTG

De in Nederland geplaatste database die binnen de CTG in 2016 is opgericht, betreft een nieuwe vorm van multilaterale gegevensuitwisseling, waaraan de AIVD bijdraagt. De CTIVD heeft zich afgevraagd hoe dit zich verhoudt tot de bepalingen in de Wiv 2002 (en de Wiv 2017).

Er kan een onderscheid worden gemaakt tussen enerzijds de gegevens in de database en anderzijds het systeem van de database. Het is een algemeen uitgangspunt in de samenwerking tussen inlichtingen- en veiligheidsdiensten dat de dienst die de gegevens verstrekt verantwoordelijk is voor de rechtmatigheid en kwaliteit van de gegevens en de nationale wet- en regelgeving van die dienst daarbij van toepassing is. De vraag is echter aan de orde wie verantwoordelijk is voor de gegevens nadát deze zijn verstrekt en in de database beschikbaar zijn. Ook m.b.t. het systeem van de database doet de vraag zich voor wie daarvoor verantwoordelijk is en welke wet- en regelgeving daarbij van toepassing zijn. Het lijkt voor de hand te liggen dat de dienst die het systeem heeft ontwikkeld en onderhoudt, de AIVD, deze verantwoordelijkheid draagt. Hier komt de vraag aan de orde of dit betekent dat de Wiv 2002 (en straks de Wiv 2017) onverkort van toepassing is op het systeem van de database.

De CTIVD heeft de juridische grondslag en verantwoordelijkheidsverdeling m.b.t. de database nader onderzocht en komt, mede op basis van het deskundigenbericht (zie bijlage IV), tot de volgende overwegingen.

---

[21] Op andere onderzoeksterreinen kan die afweging geheel anders liggen.

Gegevens in de database

De persoonsgegevens die in de database staan, betreffen in feite uitgewisselde persoonsgegevens.

Per gegeven is inzichtelijk van welke dienst de gegevens afkomstig zijn, dat wil zeggen welke dienst de gegevens aan de database heeft toegevoegd. De dienst die de gegevens heeft verstrekt is ervoor verantwoordelijk dat de verstrekte gegevens rechtmatig zijn verkregen. Men zou kunnen stellen dat de systematiek van het uitwisselen van persoonsgegevens via de database daarmee nauwelijks verschilt van andere wijzen van gegevensuitwisseling, zoals het multilateraal toesturen en ontvangen van berichten met daarin persoonsgegevens. Het gaat in feite om dezelfde (soort) gegevensuitwisseling en dezelfde kring van diensten waaraan wordt verstrekt.

Wat de gegevensuitwisseling in dit verband echter anders maakt, is allereerst dat de persoonsgegevens worden opgeslagen in een database. De persoonsgegevens zijn na toevoeging vrijwel direct beschikbaar voor alle deelnemende diensten en blijven voor hen real-time beschikbaar. Het zijn daarmee persoonsgegevens die aan alle 30 deelnemende diensten zijn verstrekt en dus na verstrekking aan alle 30 toebehoren. De persoonsgegevens zijn weliswaar ingebracht door één van de deelnemende diensten (de oorspronkelijke 'data-eigenaar'), maar zijn uitgewisseld met hen allen.

Er bestaat een verantwoordelijkheid zorg te dragen voor de persoonsgegevens die in de database zijn ingebracht, bijvoorbeeld voor de juistheid en actualiteit daarvan. Dit geldt niet alleen op het moment van het verstrekken, het plaatsen van de persoonsgegevens in de database, maar juist ook daarna omdat de gegevens *real-time* beschikbaar zijn en blijven voor alle deelnemende diensten. Ook op dit punt verschilt de gegevensuitwisseling via de database met andere, meer traditionele vormen van gegevensuitwisseling.

Wat de gegevensuitwisseling verder anders maakt, hangt samen met de dynamiek die het gebruik van de database met zich meebrengt. Zo vindt de multilaterale uitwisseling van persoonsgegevens sneller en makkelijker plaats dan voorheen. Het leidt er bovendien toe dat alle gegevens m.b.t. een persoon gecentreerd beschikbaar zijn. Dit maakt het gebruik van de gegevens in het (eigen) inlichtingenproces makkelijker en directer.

Juridisch gezien kan deze dynamiek ook zijn betekenis hebben. Het in de database samenvoegen van gegevens m.b.t. een persoon en het eventueel nader gezamenlijk analyseren daarvan, maakt dat een grotere inmenging in het recht op privacy plaatsvindt in het kader van de samenwerking dan wanneer de gegevens enkel gedeeld worden. Bij het enkel delen van gegevens vindt die inmenging immers ten dele plaats buiten de samenwerking, in de nationale context waarvoor nationale waarborgen gelden. Daar komt bij dat een database waarin gegevens uit meerdere bronnen worden verzameld, kan werken als een 'force multiplier': door gegevens te poolen kunnen inbreuken grotere effecten sorteren. Nu de inmenging die in het kader van de multilaterale samenwerking plaatsvindt groter is, dienen daarvoor ook adequate waarborgen te gelden in het kader van die samenwerking.

Verantwoordelijkheid voor de gegevens in de database

De vraag doet zich voor wie verantwoordelijk is voor de via de database uitgewisselde gegevens en wie verantwoordelijk is voor de gegevensbescherming die daarbij aan de orde moet zijn. Welk rechtsregime is daarop van toepassing? Wie houdt daar vervolgens toezicht op?

Volgens het deskundigenbericht (zie bijlage IV) staat het internationaal recht niet in de weg aan een informeel samenwerkingsverband tussen inlichtingen- en veiligheidsdiensten in het kader waarvan gegevensuitwisseling plaatsvindt. Het is informeel omdat het is gebaseerd op afspraken waaraan elke partij zich committeert maar die juridisch niet bindend zijn. Het in dit geval ontbreken van een formeel publiekrechtelijk kader, zoals een verdrag waarin bevoegdheden en verantwoordelijkheden van de deelnemende partijen expliciet zijn toebedeeld aan bijvoorbeeld een internationaal orgaan,

heeft echter een keerzijde. Het maakt dat de aan de CTG deelnemende diensten *gezamenlijke verantwoordelijkheid* dragen voor de opslag en verwerking van persoonsgegevens die in de database plaatsvindt.

De gezamenlijke verantwoordelijkheid vraagt naar het oordeel van de CTIVD om heldere afspraken over de uitwisseling, opslag en verwerking van gegevens en de bevoegdheden en plichten van elke deelnemende partij, waaronder de gegevensbescherming die gezamenlijk geboden moet worden. Het is noodzakelijk voor elk van de 30 deelnemende diensten dat hen duidelijk is wat de verantwoordelijkheid die zij gezamenlijk dragen precies inhoudt. De gezamenlijke verantwoordelijkheid kan er immers toe leiden dat wanneer sprake is van een schending van gegevensbescherming, elk van de deelnemende diensten daarop kan worden aangesproken (hoofdelijke aansprakelijkheid).

Bij die aansprakelijkheid speelt overigens het rechtens erkende vertrouwensbeginsel wel een belangrijke rol. De samenwerkende diensten mogen er, tenzij voldoende concrete omstandigheden het tegendeel aangeven, op vertrouwen dat zij zich elk houden aan de voor hen geldende wet- en regelgeving en internationale verplichtingen.[22] Dit heeft niet alleen betrekking op de wijze waarop persoonsgegevens die in de database worden ingebracht zijn verzameld, maar ook op de verdere verwerking van die gegevens. De samenwerkende diensten mogen van elkaar verwachten dat zij gemeenschappelijke standaarden naleven, onder meer op het terrein van gegevensbescherming. Dit vertrouwensbeginsel kan derhalve een mitigerende werking hebben op ieders aansprakelijkheid in het geval de rechten van een individu worden geschonden door een samenwerkingspartner. Hoofdelijke aansprakelijkheid voor het geheel kan pas aan de orde zijn indien sprake is van concrete aanwijzingen dat het vertrouwensbeginsel werd geschonden. Om het vertrouwensbeginsel te kunnen inroepen, dienen die gemeenschappelijke standaarden echter wel nadrukkelijk te zijn benoemd binnen het samenwerkingsverband.

In het deskundigenbericht (zie bijlage IV) wordt aangegeven dat gemeenschappelijke standaarden voor gegevensbescherming dienen te worden ontleend aan o.a. de algemene beginselen die zijn neergelegd in het EU-handvest, het Europees Verdrag voor de Rechten van de Mens (EVRM), Conventie 108 en de jurisprudentie van de hoven in Luxemburg en Straatsburg. Algemene beginselen voor gegevensbescherming hebben doorgaans een vertaling gekregen in nationale wetgeving die de activiteiten van inlichtingen- en veiligheidsdiensten regardeert. Het gaat hierbij onder meer om de uitgangspunten dat de verwerking van persoonsgegevens noodzakelijk is voor een bepaald legitiem doel, proportioneel is en met zorgvuldigheid wordt vormgegeven. Dat laatste houdt o.m. in dat de gegevensverwerking adequaat, relevant, accuraat en up to date is. Ook andere beschermingsmechanismen zijn van belang, zoals de instelling van een bewaartermijn, de bescherming van bijzondere categorieën persoonsgegevens, het nemen van technische en organisatorische maatregelen voor de beveiliging van persoonsgegevens en het zorgdragen voor compliance. Daarnaast worden waarborgen benoemd met betrekking tot onafhankelijk, adequaat en effectief toezicht. Het deskundigenbericht stelt dat toezicht een fundamenteel onderdeel is van de gegevensbescherming die aan de orde dient te zijn.

Het is noodzakelijk dat bovengenoemde beginselen van gegevensbescherming concreet worden ingevuld binnen de CTG-samenwerking. Voor welk doel worden gegevens in de CTG-database opgenomen en onder welke omstandigheden wordt dit door de diensten gezamenlijk noodzakelijk geacht? Welke mate van dreiging dient uit te gaan van de activiteiten van een persoon, om in verhouding te staan tot de inmenging in iemands recht op privacy? Hoe worden in deze context de begrippen adequaat, relevant, accuraat en up to date ingevuld? Ook het vermenigvuldigend effect (*force multiplier*) is van belang, zoals hiervoor al is opgemerkt. Door gegevens afkomstig van verschillende diensten

[22] Zie in dit verband Burgers t. Plasterk, ECLI:NL:GHDHA:2017:535.

samen te voegen en eventueel gezamenlijk te analyseren, kan in het kader van de samenwerking een grotere inmenging ontstaan in de privacy van personen wiens gegevens het betreft, dan wanneer de gegevens los van elkaar in de nationale context worden beschouwd. Dit dynamische proces vraagt om aanvullende waarborgen.

Het is dus van belang dat de aan de CTG deelnemende diensten gezamenlijk bepalen op welke wijze wordt voorzien in adequate rechtsbescherming en welke waarborgen daarbij aan de orde moeten zijn ontleend aan de algemene beginselen van gegevensbescherming. Daarbij dient sprake te zijn van een niveau van gegevensbescherming dat ten minste equivalent is aan het beschermingsniveau geboden door het EVRM. Ook waar het gaat om mogelijkheden voor onafhankelijk, adequaat en effectief toezicht. Gebeurt dit niet of onvoldoende, dan kunnen risico's voor toekomstig onrechtmatig handelen ontstaan (zie in dit verband paragraaf 8).

Verantwoordelijkheid voor het systeem van de database

Het systeem van de database is door de AIVD gebouwd, in samenspraak met enkele andere CTG-diensten. De server waarop de gegevens zijn opgeslagen staat in Nederland. Ook hier doet de vraag zich voor wie verantwoordelijk is, niet zozeer voor de gegevensuitwisseling maar voor de kwaliteit van het systeem dat dit mogelijk maakt. Kwaliteit wil zeggen de goede werking van het systeem en de gegevensbescherming die in dat systeem verankerd moet zijn. Is dit een collectieve verantwoordelijkheid van de CTG-diensten of een verantwoordelijkheid van de AIVD? Welk rechtsregime is daarop van toepassing? Wie houdt daar vervolgens toezicht op?

Voor de beantwoording van deze vragen geldt, blijkens het deskundigenbericht, dezelfde lijn als hierboven geschetst. Omdat geen sprake is van formele, juridisch bindende afspraken waarin verantwoordelijkheden expliciet worden toebedeeld, geldt een gezamenlijke verantwoordelijkheid van de deelnemende partijen. De CTG-diensten zijn dus in beginsel gezamenlijk verantwoordelijk voor de kwaliteit van het systeem. Dit vraagt om heldere vastlegging wat de deelnemende diensten hieronder verstaan en op welke wijze daarbij invulling wordt gegeven aan gegevensbescherming.

Voor zover de verantwoordelijkheid voor de kwaliteit van de database door de CTG-diensten informeel is toebedeeld aan de AIVD, gaat het hier om een afgeleide verantwoordelijkheid. De verantwoordelijkheid blijft bij de samenwerkende diensten gezamenlijk (dus ook de AIVD); de AIVD kan slechts worden belast met de uitvoering. In het gegevensbeschermingsrecht wordt een dergelijke partij ook wel 'bewerker' genoemd: een partij die ten behoeve van de verantwoordelijken (de 30 samenwerkende diensten) bepaalde gegevensverwerking uitvoert. Het is daarbij wel zaak dat sprake is van een duidelijke instructie of gemeenschappelijk kader aan de hand waarvan de bewerker (de AIVD) zijn afgeleide verantwoordelijkheid m.b.t. de kwaliteit van het systeem invult. Ontbreekt dit, dan moet de AIVD in de eerste plaats dit zelf invullen. Dit betekent dat de AIVD ervoor moet zorgen dat het systeem goed werkt en dat in het systeem voldoende waarborgen voor gegevensbescherming verankerd zijn. Wil men voorkomen dat de AIVD dit eenzijdig moet invullen, dan is het noodzakelijk dat de samenwerkende diensten gezamenlijk voorzien in een gemeenschappelijk kader voor de kwaliteit van het systeem.

In aanvulling daarop komt een bijzondere rol toe aan de AIVD vanwege zijn feitelijke controle en invloed op de database. De AIVD heeft als feitelijke beheerder van de database een directere betrokkenheid in het geheel dan elke andere deelnemende dienst. Dit impliceert dat de AIVD eerder kan worden aangesproken op nalatigheid met betrekking tot het waarborgen van algemene beginselen van gegevensbescherming dan een niet-beheerder. Op de AIVD rust daarom een zorgplicht: een inspanningsverplichting de bescherming van persoonsgegevens te borgen en inbreuken te voorkomen. Dit betekent niet alleen dat de inrichting van het systeem moet voorzien in voldoende rechtswaarborgen (zie hierboven), maar ook dat de AIVD de werking daarvan in de praktijk moet controleren.

Betekenis hiervan voor de AIVD

De gezamenlijke verantwoordelijkheid van alle aan de CTG-deelnemende diensten brengt met zich mee de noodzaak te voorzien in een gemeenschappelijk ingevuld kader voor gegevensbescherming. Met andere woorden, het is van belang dat de samenwerkende diensten gezamenlijk bepalen welke concrete waarborgen zij instellen voor de bescherming van de rechten van het individu. De algemene beginselen van gegevensbescherming zijn hiervoor leidend. De AIVD draagt deze verantwoordelijkheid, net als de andere 29 CTG-diensten. Dit betekent dat de AIVD zich moet inspannen een adequaat niveau van gegevensbescherming te realiseren m.b.t. de CTG database.

Waar het gaat om de beheerdersverantwoordelijkheid van de AIVD en de zorgplicht die op de dienst rust, geldt dat de AIVD zelf in voldoende rechtswaarborgen moet voorzien. Dit betekent dat in de eerste plaats gekeken kan worden naar de wijze waarop de nationale wet hiervoor een kader geeft.

In de hoofdstukken 6 en 8 en in Bijlage II wordt geconcretiseerd welke waarborgen voor gegevensbescherming voortvloeien uit de Wiv 2002 (en straks de Wiv 2017) en hoe dit zijn vertaalslag kan krijgen in multilaterale afspraken, intern beleid en te nemen maatregelen m.b.t. de kwaliteit van het systeem.

Betekenis hiervan voor het toezicht op de database

Het hebben van een gezamenlijke verantwoordelijkheid vraagt ook om gezamenlijk, multilateraal toezicht. Elk van de nationale toezichthouders komt immers voor de vraag te staan of de dienst waarop zij toezicht houdt voldoende invulling geeft aan de gezamenlijke verantwoordelijkheid die de desbetreffende dienst draagt. Nationaal toezicht alleen is dan niet voldoende. Dat sprake dient te zijn van multilateraal toezicht is recent ook door de regering onderschreven.[23] Van multilateraal toezicht op de samenwerking binnen de CTG is momenteel echter geen sprake.

In belangrijke mate zal de toezichthouder de gegevensuitwisseling en nadere verwerking vanuit het eigen mandaat en het nationale wettelijk kader beoordelen. Dit neemt niet weg dat hier nadrukkelijk ook een gezamenlijkheid aan te pas komt die nadere inbedding verdient. Het is daarom noodzakelijk dat ook de waarborg van onafhankelijk, adequaat en effectief *gezamenlijk* toezicht een plek krijgt in een gemeenschappelijk kader voor gegevensbescherming m.b.t. de CTG database.

Voor gezamenlijk toezicht zijn verschillende inrichtingswijzen denkbaar. Zo kan worden gekozen voor een beperkte samenwerking tussen toezichthouders, waarbij ieders nationale toezicht aan de hand van het eigen nationale mandaat de basis vormt. De CTIVD wijst in dit verband op de samenwerking die al plaatsvindt tussen een vijftal toezichthouders in een gezamenlijk project over de gegevensuitwisseling m.b.t. (vermeende) jihadisten. Een beperking is hierbij wel dat de toezichthouders elk zijn gebonden aan een wettelijke geheimhoudingsplicht, die eraan in de weg staat onderling te spreken over zaken die als staatsgeheim zijn aangemerkt. Dit leidt er bijvoorbeeld toe dat inhoud van de multilaterale afspraken die binnen de CTG zijn gemaakt, en die voor elk van de diensten gelden, niet door de nationale toezichthouders besproken kunnen worden. Een verdergaande vorm van samenwerking tussen toezichthouders zou daarom noodzakelijk zijn, waarbij dergelijke beperkingen terzijde worden geschoven. Dit dient dan wel een inbedding te krijgen in een gemeenschappelijk kader voor gegevensbescherming.

Een andere mogelijkheid zou zijn te komen tot een expliciete verdeling van toezichtstaken, waarbij een of enkele toezichthouders de taak krijgen invulling te geven aan het gezamenlijke toezicht. Hier kan een parallel worden getrokken met de verhouding tussen de 'verantwoordelijke(n)' en de 'bewerker' in het gegevensbeschermingsrecht. Een of enkele toezichthouders zouden de verantwoordelijkheid kunnen

---

[23] Antwoorden op Kamervragen gesteld door het lid Verhoeven, *Aanhangsel Handelingen II* 2017/18, nr. 202..

krijgen om namens hen allen gezamenlijk toezicht uit te oefenen. Ook hier zou een gemeenschappelijke kader of een instructie aan ten grondslag moeten liggen. De verantwoordelijken blijven daarin leidend.

Een derde vorm betreft overkoepelend, internationaal toezicht. Hierbij zou een nieuwe internationale toezichtsinstantie in het leven worden geroepen waaraan bepaalde toezichtsbevoegdheden worden toegekend. Dit is de meest vergaande vorm en vereist een publiekrechtelijke grondslag in bijvoorbeeld een verdrag tussen staten. Nu de multilaterale samenwerking tussen inlichtingen- en veiligheidsdiensten niet is gebaseerd op formeel bindende afspraken maar op informele afspraken, lijkt een dergelijke inrichting voor gezamenlijk toezicht niet direct passend.

5.5.3 Juridische grondslag sigint samenwerking

In het kader van de onderzochte multilaterale samenwerking op het terrein van sigint is sprake van zowel gezamenlijke gegevensverwerking als het in gezamenlijkheid uitoefenen van (bijzondere) bevoegdheden.

Gezamenlijke gegevensverwerking

Waar binnen de sigint samenwerking sprake is van gezamenlijke gegevensverwerking, zoals de opslag van uitgewisselde gegevens, gelden dezelfde overwegingen als die hierboven m.b.t. de CTG database zijn weergegeven. De gezamenlijke gegevensverwerking vindt, bij het ontbreken van formeel bindende afspraken, plaats onder de gezamenlijke verantwoordelijkheid van de deelnemende diensten. Zij dienen met elkaar te voorzien in een adequaat niveau van gegevensbescherming. De CTIVD constateert dat hierin in belangrijke mate is voorzien. In paragraaf 6.4 en hoofdstuk 8 bespreekt de CTIVD op welke punten nog sprake is van onvoldoende waarborgen en welke risico's daarbij aan de orde kunnen komen.

De gezamenlijke verwerking van gegevens op het terrein van sigint kan samenhangen met de gezamenlijke uitoefening van (bijzondere) bevoegdheden. Hiervoor hanteert de CTIVD een aanvullend kader. Dit wordt hieronder besproken.

Gezamenlijke uitoefening bevoegdheden

De CTIVD heeft zich de vraag gesteld of sprake is van een juridische basis voor het onder gezamenlijke verantwoordelijkheid uitoefenen van bepaalde bevoegdheden, resulterend in gezamenlijke (sigint) inlichtingenproducten.

Zoals in paragraaf 5.3 is aangegeven geeft de Wiv 2002 (en de Wiv 2017) een algemene grondslag voor de samenwerking door de AIVD met buitenlandse diensten en specifieke bepalingen voor de verstrekking van (persoons)gegevens en het verlenen van ondersteuning. Voor het onder gezamenlijke verantwoordelijkheid uitoefenen van bevoegdheden is geen specifieke regeling getroffen.

De CTIVD is van oordeel dat het de AIVD (en de MIVD) op basis van de algemene bevoegdheid tot samenwerking met buitenlandse diensten in beginsel is toegestaan in de samenwerking te komen tot een *division of effort*, dat wil zeggen een verdeling van taken en inzet van menskracht en middelen. Dit kan ook inhouden dat een bepaalde bevoegdheid in gezamenlijkheid wordt uitgevoerd, onder gezamenlijke verantwoordelijkheid. Voorwaarden zijn wel dat:

1. de AIVD de bevoegdheid die wordt uitgeoefend zelf geniet;
2. de daar op van toepassing zijnde wet- en regelgeving (o.a. de Wiv 2002) wordt nageleefd;
3. geen sprake is van het systematisch of willens en wetens ontvangen van gegevens van buitenlandse diensten, die de AIVD (of de MIVD) niet op grond van eigen bevoegdheden kan vergaren;[24] en
4. effectief toezicht mogelijk is.

Deze voorwaarden zorgen ervoor dat dezelfde mate van rechtsbescherming wordt geboden in de samenwerking met buitenlandse diensten als in de nationale context.

Op dit moment voldoet de betrokkenheid van de AIVD bij de multilaterale sigint samenwerking aan de eerste drie voorwaarden. De CTIVD ziet hier dan ook geen strijdigheid met de Wiv 2002, in tegendeel. De multilaterale afspraken die in dat kader zijn gemaakt, vormen zelfs aanvullende waarborgen dat de genoemde voorwaarden worden toegepast. De CTIVD ziet m.b.t. de tweede voorwaarde, de naleving van de nationale wet- en regelgeving, wel een moeilijkheid ontstaan met de inwerkingtreding van de nieuwe Wiv 2017. De Wiv 2017 geeft een strikter kader voor onderzoeksopdrachtgerichte interceptie en de verdere verwerking van de geïntercepteerde gegevens dan nu aan de orde is bij de ongerichte interceptie onder de Wiv 2002. Zij gaat hier in het geheime toezichtsrapport nader op in.

Over de vierde voorwaarde, de mogelijkheid tot het uitoefenen van effectief toezicht, zijn binnen de multilaterale sigint samenwerking voor bepaalde vormen van samenwerking afspraken gemaakt. Deze afspraken komen voor het toezicht door de CTIVD erop neer dat zij zich kan richten op de uitoefening van bevoegdheden door de AIVD en in beperkte mate op het gebruik door andere deelnemende diensten van gegevens die door de AIVD zijn verstrekt. Er wordt echter aan de nationale toezichthouders op dit punt een beperking opgelegd. Deze beperking is van dien aard dat het nationale toezicht daarmee niet volledig effectief is. De CTIVD vindt het noodzakelijk dat wordt voorzien in gezamenlijk toezicht op het gebruik van de gegevens. In paragraaf 5.5.2 zijn hier verschillende invullingsrichtingen voor gegeven. Het is daarnaast van belang dat dit toezicht ook technisch mogelijk wordt gemaakt.

Het is verder noodzakelijk dat effectief toezicht plaats kan vinden op de vernietiging van de door de AIVD verstrekte gegevens. Deze mogelijkheid is voorzien in multilaterale afspraken maar nog niet gerealiseerd.

[24] Dit element vloeit voort uit het arrest Burgers t. Plasterk, ECLI:NL:GHDHA:2017:535.

6 Waarborgen

6.1 Inleiding

De CTIVD heeft onderzocht in hoeverre bij de multilaterale gegevensuitwisseling m.b.t. (vermeende) jihadisten door de AIVD invulling wordt gegeven aan de wettelijke waarborgen voor de bescherming van grondrechten. In de Wiv 2002 (en de Wiv 2017) zijn daarvoor vier vereisten neergelegd: noodzakelijkheid, behoorlijkheid, zorgvuldigheid en (aanduiding van) betrouwbaarheid. In bijlage II bij dit rapport wordt uiteengezet wat onder elk vereiste verstaan moet worden in het kader van multilaterale gegevensuitwisseling. Hieronder in paragraaf 6.2 wordt dit schematisch weergegeven.

In dit hoofdstuk wordt verder beschreven in hoeverre deze waarborgen hun vertaling hebben gekregen in multilaterale afspraken binnen de CTG en de sigint samenwerking of in intern beleid van de AIVD. Ook heeft de CTIVD (steekproefsgewijs) getoetst of de AIVD de gemaakte afspraken in de praktijk nakomt. De bevindingen van de CTIVD zijn in de paragrafen 6.3 en 6.4 samengevat weergegeven. In bijlage II worden de bevindingen van de CTIVD meer in detail beschreven. Het is de CTIVD niet toegestaan in dit openbare rapport uitgebreid in te gaan op de inhoud van multilaterale afspraken, vanwege het staatsgeheime karakter daarvan. In het geheime toezichtsrapport wordt daar wel nader op ingegaan.

Op basis van deze bevindingen trekt de CTIVD conclusies over de uitvoeringspraktijk op dit moment. Deze conclusies staan beschreven in hoofdstuk 7 van het toezichtsrapport. Waar waarborgen voor gegevensbescherming ontbreken of (nog) onvoldoende stevig verankerd zijn, is sprake van risico's voor toekomstig onrechtmatig handelen. Dit bespreekt de CTIVD in hoofdstuk 8 van het toezichtsrapport.

6.2 Waarborgen voor multilaterale gegevensuitwisseling

Noodzakelijkheid	• Is sprake van een heldere definiëring van de gevallen waarin tot gegevensuitwisseling of -analyse kan worden overgegaan (drempel)?
Behoorlijkheid	• Staat het gewicht van de inmenging in grondrechten die plaatsvindt in verhouding tot het gewicht van de (operationele) belangen die worden gediend? Het gewicht van de inmenging wordt bepaald door: – het aantal diensten waaraan wordt verstrekt; – het gebruik van de verstrekte gegevens; – de hoeveelheid en gevoeligheid van de gegevens. Het gewicht van de operationele belangen wordt bepaald door de prioritering van het target.
Zorgvuldigheid	• Zijn de verwerkte persoonsgegevens correct weergegeven, juist (d.w.z. onderbouwd en actueel), schriftelijk verstrekt, nog relevant? Worden gegevens vernietigd wanneer dit niet (meer) het geval is? • Zijn de nodige voorzieningen getroffen ter bevordering van de juistheid en de volledigheid van de gegevens die worden verwerkt?
Betrouwbaarheid	• Is sprake van een aanduiding van de betrouwbaarheid? • Zijn de nodige voorzieningen getroffen van technische en organisatorische aard op het gebied van gegevensbeveiliging?

6.3 Waarborgen voor de gegevensuitwisseling door de AIVD binnen de CTG

Noodzakelijkheid

Om de noodzakelijkheid van de gegevensuitwisseling te waarborgen, is een duidelijke definiëring van de gevallen waarin tot gegevensuitwisseling kan worden overgegaan van belang. Die definiëring dient een drempel te vormen voor gegevensuitwisseling.

Bij de bijeenkomsten van het operationeel platform is sprake van een noodzakelijkheidsdrempel, doordat bij elke casus die daar besproken wordt tot dusver op voorhand een duidelijke afbakening plaatsvindt van de groep personen waarop de operationele gegevensuitwisseling zich kan richten. De persoonsgegevens die door de AIVD worden verstrekt, vallen binnen die afbakening.

De AIVD maakt zelf de afweging m.b.t. welke personen gegevens worden uitgewisseld via de CTG database. Binnen de AIVD bestond het uitgangspunt dat de dienst uitsluitend gegevens van daadwerkelijk uitgereisde of zeer hoog geprioriteerde niet uitgereisde personen verstrekte. Deze lijn is begin 2017 losgelaten. In beleid van augustus 2017 is opgenomen dat het moet gaan om “geduide contra terrorisme targets”. De CTIVD vindt dat deze definiëring van beperkte betekenis is. Het is dermate algemeen dat het de kring van personen over wie gegevens worden gedeeld onvoldoende beperkt. Het vormt een weinig betekenisvolle drempel voor gegevensuitwisseling via de CTG database.

De CTIVD heeft echter geen concrete gevallen aangetroffen waarbij de gegevensverstrekking door de AIVD niet noodzakelijk was. Wel ziet zij sinds begin 2017 een verschuiving in het ‘type’ targets wiens persoonsgegevens via de database worden gedeeld door de AIVD.

De CTIVD ziet risico’s in het geval de drempel voor gegevensuitwisseling lager wordt. Zij bespreekt dit in hoofdstuk 8.

Behoorlijkheid

Het gewicht van de inmenging in de grondrechten van de personen wiens gegevens worden verstrekt, kan aanzienlijk zijn, met name door het aantal diensten waaraan wordt verstrekt. Waarborgen daarbij zijn noodzakelijk. Zo is het van belang het gebruik van de gegevens die zijn verstrekt en de doorverstrekking daarvan aan derden te limiteren. Ook kunnen aanvullende waarborgen worden ingesteld voor de uitwisseling van gevoelige gegevens of bepaalde categorieën personen, zoals minderjarigen.

Tegenover de inmenging in grondrechten staat het operationeel belang met betrekking tot de gegevensverstrekking. Het is noodzakelijk te waarborgen dat aan elk target dat aan de database wordt toegevoegd, een voldoende hoog operationeel belang is toegekend. Dit wordt ook wel de prioritering van het target genoemd.

De gegevensuitwisseling door de AIVD is vooralsnog behoorlijk te noemen. Gegevens worden uitsluitend gebruikt ten behoeve van het inlichtingenproces en onder strikte regels doorverstrekt aan derden. Wat betreft de hoeveelheid van gegevens per target en de gevoeligheid daarvan, is de gegevensverstrekking door de AIVD beperkt. Voor de verstrekking van gegevens m.b.t. minderjarigen zijn door de AIVD geen aanvullende waarborgen ingesteld. De CTIVD ziet hier het belang aanvullende waarborgen in te richten. Zij bespreek dit verder in hoofdstuk 8.

Over de wijze waarop prioritering van targets plaatsvindt heeft de AIVD intern beleid opgesteld. De personen wiens gegevens door de AIVD zijn verstrekt hebben doorgaans een hoge prioritering, onder meer gelet op de dreiging die van deze personen uitgaat. De CTIVD constateert wel dat hierin vanaf begin 2017 een verschuiving is opgetreden.

Zorgvuldigheid

Het is voor de zorgvuldigheid van de gegevensuitwisseling van belang dat voorwaarden gelden voor de correcte weergave, de onderbouwing, het actueel houden en het tijdig vernietigen van de uitgewisselde gegevens.

In de database zijn systeemtechnische voorzieningen getroffen die de juistheid en volledigheid van de gegevensuitwisseling bevorderen. De database voorziet niet in mechanismen voor het actueel houden van de gegevens en het tijdig vernietigen daarvan. De CTIVD ziet hier verschillende mogelijkheden voor de AIVD bestaande waarborgen te versterken of aanvullende waarborgen in te richten. Zij bespreekt dit verder in hoofdstuk 8.

De CTIVD heeft slechts enkele gevallen aangetroffen waarbij de gegevensverstrekking door de AIVD via de CTG database op onderdelen onzorgvuldig is geweest. Het betrof hier een verschil tussen de persoonsgegevens in de eigen nationale systemen en de CTG database. De desbetreffende persoonsgegevens in de database waren onvoldoende volledig of nog niet geactualiseerd. Dit is inmiddels hersteld.

De gegevensuitwisseling die plaatsvindt tijdens de bijeenkomsten van het operationeel platform wordt vastgelegd in verslagen. De CTIVD ziet m.b.t. het mondeling verstrekken van persoonsgegevens bepaalde risico's. Dit wordt besproken in hoofdstuk 8.

Betrouwbaarheid

Op het punt van betrouwbaarheid van de uitgewisselde gegevens dient een bepaald minimum betrouwbaarheidsniveau of een betrouwbaarheidsindicatie aan de orde te zijn.

In de database wordt de mogelijkheid geboden onzekere gegevens een rood kenmerk te geven. Ook zijn door de AIVD de nodige voorzieningen getroffen ter beveiliging van de gegevens tegen verlies of aantasting of tegen onbevoegde gegevensverwerking. Het systeem waarborgt onder meer dat (met uitzondering van de beheerder van de database) uitsluitend de dienst die de gegevens inbrengt, die gegevens kan wijzigen. De CTIVD heeft geen twijfel dat sprake is van een betrouwbaar systeem. Voor de toegang tot het systeem en de mogelijkheid om gegevens toe te voegen, zijn geen nadere beperkingen gesteld.

Voor de gegevens die de AIVD zelf verstrekt, is wettelijk vereist dat deze zijn voorzien van een betrouwbaarheidsindicatie of een bronverwijzing. Hierin wordt door de AIVD niet voorzien. Evenmin is intern vastgelegd dat de AIVD alleen volledig betrouwbare gegevens verstrekt via de database of binnen het operationeel platform. De CTIVD heeft steekproefsgewijs getoetst wat de betrouwbaarheid c.q. herkomst is van de door de AIVD verstrekte gegevens in de database en het operationeel platform. Dit heeft niet geleid tot indicaties dat de verstrekte gegevens onvoldoende betrouwbaar zijn.

6.4 Waarborgen voor de gegevensuitwisseling door de AIVD binnen de sigint samenwerking

Noodzakelijkheid

Het is inherent aan de uitwisseling van ongeëvalueerde gegevens dat de noodzakelijkheid daarvan slechts in algemene bewoordingen en op hoofdlijnen kan worden vastgesteld. Een vastomlijnde definiëring van de jihadisten met betrekking tot wie gegevens worden verstrekt is niet mogelijk wanneer men op voorhand niet weet op welke personen de gegevens betrekking hebben. De noodzakelijkheidsdrempels die hier aan de orde moeten zijn, kunnen dan ook niet één op één worden vergeleken met de noodzakelijkheidsdrempels voor de uitwisseling van geëvalueerde gegevens. Multilaterale afspraken binnen de sigint samenwerking geven invulling aan het noodzakelijkheidsvereiste.

Behoorlijkheid

Multilaterale afspraken binnen de sigint samenwerking waarborgen in belangrijke mate dat de doorverstrekking en het gebruik van de uitgewisselde gegevens wordt beperkt.

Waar het gaat om het vaststellen van het gewicht van de inmenging in de grondrechten van de personen wiens gegevens de AIVD heeft verstrekt, heeft de waarborg van behoorlijkheid beperkte betekenis bij het uitwisselen van ongeëvalueerde gegevens (in bulk). Het is op voorhand niet duidelijk wiens persoonsgegevens worden verstrekt. De inmenging in grondrechten is daarmee niet goed in kaart te brengen. Wel kan aan de hand van de hoeveelheid en de aard van de gegevens de inmenging in algemene zin worden bepaald. De andere kant van de weegschaal, het belang van het uitwisselen van de gegevens voor de internationale bestrijding van het jihadisme, is evenmin concreet te duiden. Ook dit kan slechts in algemene zin. In algemene zin is in de onderhavige multilaterale sigint samenwerking het gewicht van de inmenging beperkt en is sprake van heldere afspraken omtrent de doorverstrekking en het gebruik van de gegevens.

Omdat de behoorlijkheidsafweging niet goed op het individuele target gemaakt worden, vormt de vereiste toestemming van de minister voor het uitwisselen van ongeëvalueerde gegevens een belangrijke aanvullende waarborg. De minister dient af te wegen of hij de risico's die gepaard gaan met de uitwisseling aanvaardbaar acht, mede gelet op het belang van de uitwisseling. Het gaat hier vooral om het risico dat de AIVD niet precies weet welke gegevens hij deelt en dus niet de consequenties kan overzien van het gebruik van die gegevens door de buitenlandse diensten in kwestie. De minister beoordeelt of hij dit risico in een specifiek geval aanvaardbaar acht en dient daarbij te toetsen aan de in de wegingsnotities gestelde kaders. Het is dan wel van wezenlijk belang dat er wegingsnotities zijn. Deze ontbreken op dit moment.

De CTIVD stelt vast dat er tussen 30 juni 2016 en 6 december 2016 geen sprake was van een geldende ministeriële toestemming voor het verstrekken van de ongeëvalueerde gegevens.

Zorgvuldigheid

Multilaterale afspraken geven invulling aan het zorgvuldigheidsvereiste bij de uitwisseling van *ongeëvalueerde* gegevens. De herkomst van de gegevens en de vernietiging daarvan zijn geborgd. Ook geldt als uitgangspunt dat gegevens schriftelijke verstrekt worden.

De multilaterale afspraken over de mogelijkheid van controle en toezicht op de zorgvuldige verwerking van gegevens binnen de sigint samenwerking zijn voor deze beoordeling van wezenlijk belang. In de praktijk is effectief toezicht vanwege technische en organisatorische redenen echter nog niet volledig mogelijk. De verwachting bestaat dat dit in 2018 wel het geval is.

Met betrekking tot één specifieke vorm van de uitwisseling van *geëvalueerde* gegevens is de zorgvuldigheid onvoldoende geborgd. Er zijn geen adequate waarborgen die ervoor zorgen dat de gegevens correct zijn weergegeven, voldoende inhoudelijk onderbouwd en actueel zijn. Wel is met betrekking tot de gegevens een uiterlijke vernietigingstermijn afgesproken. In de praktijk is de herkomst van de gegevens onvoldoende inzichtelijk.

Betrouwbaarheid

De AIVD voldoet niet aan het wettelijke vereiste dat gegevens zijn voorzien van een betrouwbaarheidsindicatie of een bronverwijzing, voor zover het gaat om de verstrekking van *geëvalueerde* gegevens.

7 Conclusies

Conclusies m.b.t. de juridische grondslag

Algemene grondslag voor samenwerking

Voor de samenwerking door de AIVD in multilaterale samenwerkingsverbanden met buitenlandse inlichtingen- en veiligheidsdiensten is een basis neergelegd in de Wiv 2002. De Wiv 2002 stelt daarbij de voorwaarde dat buitenlandse diensten waarmee wordt samengewerkt, daarvoor in aanmerking moeten komen. Dit betekent dat de AIVD per buitenlandse dienst een risicoweging moet maken aan de hand van samenwerkingscriteria. Op basis van deze risicoweging wordt bepaald van welke risico's sprake is, welke vormen van samenwerking met de buitenlandse diensten op welke terreinen geoorloofd zijn en met welke intensiteit kan worden samengewerkt. Dit moet worden vastgelegd in een wegingsnotitie. Het gaat hier om een operationele, juridische en politieke afweging, die de minister van BZK uiteindelijk moet dragen en verantwoorden.

Met betrekking tot de diensten waarmee de AIVD in de onderzochte multilaterale verbanden samenwerkt (binnen CTG en op het terrein van sigint), zijn geen wegingsnotities met risicowegingen vastgesteld.

- In de eerste plaats stelt het ontbreken van een risicoweging formeel de legitimiteit van de samenwerking ter discussie. Zonder risicoweging wordt niet voldaan aan de basisvoorwaarde voor samenwerking. De CTIVD beoordeelt het ontbreken hiervan als **onrechtmatig**. Overigens is in de Wiv 2017 een bepaling opgenomen die de invoering van de systematiek van wegingsnotities met twee jaar uitstelt voor bestaande samenwerkingsrelaties. De ministers van BZK en Defensie hebben toegezegd dat bij de inwerkingtreding van de Wiv 2017 de wegingsnotities m.b.t. deze diensten reeds vastgesteld zullen zijn.

- In de tweede plaats leidt dit tot de vraag of de betrokken buitenlandse diensten materieel in aanmerking komen voor de specifieke vormen van samenwerking die door de CTIVD in dit onderzoek zijn onderzocht. De CTIVD komt tot de conclusie dat dit voor de desbetreffende diensten het geval is, gelet op het zwaarwegende belang van de internationale bestrijding van het jihadisme en de noodzaak tot intensieve samenwerking daarbij. Dit wordt ook (inter)nationaal politiek-bestuurlijk uitgedragen. Wel blijft het van rechtsstatelijk belang dat de AIVD in kaart brengt waar risico's in de samenwerking met elk van de desbetreffende buitenlandse diensten zich kunnen voordoen. Ook in het kader van de internationale bestrijding van het jihadisme moet de AIVD zich hier rekenschap van geven en waar nodig aanvullende waarborgen instellen voor de bescherming van de grondrechten van de burger.

Specifieke samenwerkingsvormen

De specifieke informele samenwerkingsvormen die onderwerp zijn van dit onderzoek, zijn gericht op intensivering van de multilaterale gegevensuitwisseling m.b.t. (vermeende) jihadisten. De samenwerkingsvormen zijn als zodanig niet expliciet voorzien in de Wiv 2002 (noch in de Wiv 2017). De wet schrijft echter niet dwingend voor op welke wijze de samenwerking en gegevensuitwisseling plaats dient te vinden en biedt daarom in beginsel ruimte hiervoor. Ook de beginselen van internationaal recht verzetten zich niet tegen het informele karakter van deze samenwerkingsverbanden.

De in 2016 opgerichte CTG database is zo'n nieuwe vorm van gegevensuitwisseling. De database staat op Nederlands grondgebied. De CTIVD heeft zich afgevraagd hoe de uitwisseling en verdere verwerking van gegevens in de database zich verhoudt tot de Wiv 2002 (en de nieuwe Wiv 2017). Mede op basis van de inhoud van het deskundigenbericht (zie bijlage IV), concludeert de CTIVD het volgende:

- Er is sprake van gezamenlijke opslag en verwerking van gegevens in de CTG database. De samenwerkende veiligheidsdiensten zijn hiervoor *gezamenlijk verantwoordelijk*. De gezamenlijke verantwoordelijkheid strekt zich uit tot de gegevens in de database, het beheer van de database en de gegevensbescherming die daarbij geboden moet worden. Dit vraagt om heldere afspraken over de gegevensuitwisseling en invulling van gemeenschappelijke standaarden die voor elke deelnemende partij gelden. De CTIVD constateert dat hierin slechts in beperkte mate is voorzien.

- Gemeenschappelijke standaarden worden ontleend aan de algemene beginselen voor gegevensbescherming. Het gaat hierbij onder meer om de uitgangspunten dat de verwerking van persoonsgegevens noodzakelijk is voor een bepaald legitiem doel, proportioneel is en met zorgvuldigheid wordt vormgegeven. Dat laatste houdt o.m. in dat de gegevensverwerking adequaat, relevant, accuraat en up to date is. Ook andere beschermingsmechanismen zijn essentieel, zoals de instelling van een bewaartermijn, de bescherming van bijzondere categorieën persoonsgegevens, het nemen van technische en organisatorische maatregelen voor de beveiliging van persoonsgegevens en het zorgdragen voor compliance. Daarnaast worden waarborgen benoemd met betrekking tot onafhankelijk, adequaat en effectief toezicht.

- Het is noodzakelijk dat deze beginselen van gegevensbescherming thans concreet worden ingevuld binnen de CTG-samenwerking. Voor welk doel worden gegevens in de CTG-database opgenomen en onder welke omstandigheden wordt dit door de diensten gezamenlijk noodzakelijk geacht? Welke mate van dreiging dient uit te gaan van de activiteiten van een persoon, om in verhouding te staan tot de inmenging in iemands recht op privacy? Hoe wordt in deze context adequaat, relevant, accuraat en up to date ingevuld? De aan de CTG deelnemende diensten dienen dus gezamenlijk te bepalen op welke wijze wordt voorzien in adequate rechtsbescherming en welke waarborgen daarbij aan de orde moeten zijn.

- Een bijzondere positie komt toe aan de AIVD, die als beheerder van de database verantwoordelijk is voor de kwaliteit van het systeem. Het is daarbij wel zaak dat sprake is van een duidelijke instructie of gemeenschappelijk kader aan de hand waarvan de AIVD zijn afgeleide verantwoordelijkheid m.b.t. het beheer van de database invult. Voor zover dit ontbreekt, moet de AIVD zelf in voldoende rechtswaarborgen voorzien. De AIVD heeft vanwege zijn feitelijke controle en invloed, een directere betrokkenheid in het geheel dan elke andere deelnemende dienst. Op de AIVD rust een zorgplicht: een inspanningsverplichting de bescherming van persoonsgegevens te borgen en inbreuken te voorkomen.

- Het specifieke karakter van deze samenwerking, waarvoor een gezamenlijke verantwoordelijkheid geldt, vraagt om *gezamenlijk toezicht*. Hierin is nu niet voorzien. Voor gezamenlijk toezicht zijn verschillende inrichtingswijzen denkbaar. Zo kan worden gekozen voor een beperkte of verdergaande samenwerking tussen toezichthouders, een expliciete verdeling van toezichtstaken of overkoepelend toezicht. Ook de waarborg van onafhankelijk, adequaat en effectief gezamenlijk toezicht dient onderdeel uit te maken van een gemeenschappelijk CTG kader voor gegevensbescherming.

In het kader van de onderzochte multilaterale samenwerking op het terrein van sigint is sprake van zowel gezamenlijke opslag en verwerking van gegevens als het in gezamenlijkheid uitoefenen van (bijzondere) bevoegdheden.

- Gezamenlijke gegevensverwerking vindt plaats onder de gezamenlijke verantwoordelijkheid van de deelnemende diensten. Zij dienen met elkaar te voorzien in een adequaat niveau van gegevensbescherming. De CTIVD constateert dat hierin in belangrijke mate is voorzien.

- Daarnaast is sprake van samenwerkingsvormen waarbij gezamenlijk (bijzondere) bevoegdheden worden ingezet. De CTIVD is van oordeel dat het de AIVD op basis van de algemene bevoegdheid tot samenwerking met buitenlandse diensten in beginsel is toegestaan te komen tot een *division of effort*, dat wil zeggen een verdeling van taken en inzet van menskracht en middelen. Dit kan ook inhouden dat een bepaalde bevoegdheid in gezamenlijkheid wordt uitgevoerd, onder gezamenlijke verantwoordelijkheid. Voorwaarden zijn wel dat:

  1. de AIVD daarbij blijft binnen de wettelijk aan de dienst toegekende bevoegdheden;
  2. de Nederlandse wet- en regelgeving wordt gevolgd waar het gaat om de deelname van de AIVD;
  3. geen sprake is van het systematisch of willens en wetens ontvangen van gegevens die de AIVD niet op grond van eigen bevoegdheden kan vergaren; en
  4. effectief toezicht daarop mogelijk is.

- Deze voorwaarden, die evenzeer voor de MIVD gelden, zorgen ervoor dat een gelijk niveau van rechtsbescherming wordt geboden in de samenwerking met buitenlandse diensten als in de nationale context. De CTIVD constateert dat door de AIVD wordt voldaan aan de eerste drie voorwaarden. Het toezicht op het gebruik van gegevens is nog onvoldoende effectief, omdat het nationale toezicht beperkt is en niet is voorzien in gezamenlijk toezicht. Het toezicht is bovendien niet effectief, doordat vanwege technische redenen momenteel geen toegang kan worden gegeven tot de benodigde gegevens. Dit zou moeten veranderen in 2018.

Conclusies met betrekking tot de uitvoeringspraktijk op dit moment

De CTIVD heeft onderzocht in hoeverre bij de gegevensuitwisseling m.b.t. (vermeende) jihadisten tussen de AIVD en buitenlandse diensten binnen de CTG en de sigint samenwerking invulling wordt gegeven aan de wettelijke waarborgen voor de bescherming van grondrechten. In de Wiv 2002 (en de Wiv 2017) zijn daarvoor vier vereisten neergelegd: noodzakelijkheid, behoorlijkheid, zorgvuldigheid en (aanduiding van) betrouwbaarheid (zie ook bijlage II).

Noodzakelijkheid

Noodzakelijkheid betekent concreet dat de AIVD bij de verstrekking van gegevens 1) een vooraf omschreven doel moet hebben dat past binnen de wettelijke taken die aan de AIVD zijn opgedragen; 2) de redelijke verwachting moet hebben dat dit doel wordt bereikt door het verstrekken van de gegevens aan de desbetreffende buitenlandse dienst(en); en 3) dit kan onderbouwen.

Het is inherent aan de uitwisseling van persoonsgegevens in een breed multilateraal verband dat de noodzakelijkheidsafweging vrijwel dezelfde is bij elk persoonsgegeven dat wordt uitgewisseld. De waarde van het noodzakelijkheidsvereiste is erin gelegen dat het een drempel vormt voor de multilaterale gegevensuitwisseling. Die drempel is hoger naarmate duidelijker is omschreven en vastgelegd mb.t. welke personen of in welke gevallen gegevensuitwisseling noodzakelijk wordt geacht. De drempel wordt lager naarmate dit algemener wordt omschreven en niet is vastgelegd. Met andere woorden, noodzakelijkheid van multilaterale gegevensuitwisseling vereist een heldere definiëring om wie of wat het gaat.

De AIVD heeft in intern beleid vastgelegd dat het bij het plaatsen van persoonsgegevens in de CTG database moet gaan om “geduide contra terrorisme targets”. Deze definiëring is dermate algemeen dat het een weinig betekenisvolle drempel vormt. Aan het noodzakelijkheidsvereiste wordt door de AIVD in de praktijk echter wel voldoende invulling gegeven. De CTIVD heeft geen door de AIVD verstrekte persoonsgegevens in de database aangetroffen waarbij de verstrekking niet noodzakelijk was. Ook blijft de AIVD binnen de afbakening die bij elke casus in het operationeel platform van de CTG wordt gehanteerd.

In het kader van de sigint samenwerking geldt een onderscheid tussen ongeëvalueerde en geëvalueerde gegevens. De drempel voor de uitwisseling van *ongeëvalueerde* gegevens ligt voldoende hoog, doordat in multilaterale afspraken invulling is gegeven aan het noodzakelijkheidsvereiste. Dit is anders waar het gaat om een specifieke vorm van uitwisseling van geëvalueerde gegevens. Daarvoor ontbreekt een heldere definiëring met betrekking tot welke personen c.q. in welke gevallen gegevens kunnen worden uitgewisseld.

Behoorlijkheid

Behoorlijkheid houdt in dat het gewicht van de inmenging in iemands grondrechten in redelijke verhouding staat tot het gewicht van de (operationele) belangen die de AIVD heeft bij de gegevensverstrekking.

Behoorlijkheid vereist waarborgen die het gebruik van de gegevens die zijn verstrekt en de doorverstrekking daarvan aan derden limiteren en de uitwisseling van gevoelige gegevens of bepaalde categorieën personen, zoals minderjarigen beperken. Ook is het noodzakelijk te waarborgen dat aan elk target waarover gegevens worden verstrekt, een voldoende hoog operationeel belang is toegekend.

De CTIVD is van oordeel dat de gegevensuitwisseling door de AIVD vooralsnog behoorlijk te noemen is. De AIVD staat de verstrekking en het gebruik van gegevens buiten het inlichtingenproces niet zonder meer toe. De gegevensverstrekking van de AIVD is in termen van hoeveelheid en gevoeligheid vooralsnog beperkt en betreft doorgaans hoog geprioriteerde targets,

Bij de uitwisseling en het gebruik van *ongeëvalueerde* gegevens in multilaterale sigint samenwerking is het behoorlijkheidsvereiste van beperktere betekenis. Behoorlijkheid kan slechts worden beoordeeld op hoofdlijnen, zonder een concreet gewicht te kunnen hangen aan een van beide zijden van de weegschaal. Juist daarom wordt als aanvullende waarborg vereist dat de minister toestemming verleent voor de uitwisseling van ongeëvalueerde gegevens. De minister moet de afweging maken of hij de risico's die daarmee gepaard gaan in het kader van de specifieke samenwerking aanvaardbaar acht. Hij dient daarbij te toetsen aan het in de wegingsnotitie(s) gestelde kader voor de samenwerking. Zonder wegingsnotitie(s), wat op dit moment het geval is, verliest deze toets aan waarde. Met betrekking tot bepaalde samenwerkingsvormen is ten minste jaarlijks toestemming van zowel de minister van BZK als de minister van Defensie vereist. Deze toestemming van beide ministers ontbrak gedurende een periode van vijf maanden. De CTIVD beoordeelt dit als **onrechtmatig**.

Zorgvuldigheid

Zorgvuldigheid is een kwaliteitsvereiste. Het heeft betrekking op correcte weergave van de gegevens en de juistheid daarvan, wat onder meer inhoudt dat de gegevens onderbouwd en actueel dienen te zijn. Persoonsgegevens moeten in beginsel schriftelijk worden verstrekt, tenzij sprake is van spoed. Waar het gaat om gegevensverwerkingsprocessen, moet sprake zijn van voorzieningen ter bevordering van de juistheid en de volledigheid van de gegevens.

In het kader van de CTG database en de uitwisseling van ongeëvalueerde gegevens binnen de sigint samenwerking is sprake van systeemtechnische waarborgen voor de correcte weergave van gegevens en duidelijkheid over de herkomst van gegevens. Ook is inzichtelijk wanneer persoonsgegevens het laatst zijn gewijzigd en door welke dienst. De AIVD draagt hier een verantwoordelijkheid als beheerder van de CTG database. De CTIVD is van oordeel dat de AIVD deze verantwoordelijkheid feitelijk voldoende heeft ingevuld, maar ziet verschillende mogelijkheden bestaande waarborgen te versterken.

De zorgvuldigheid van de gegevensverstrekking door de AIVD is afhankelijk van de standaarden die de dienst daarvoor zelf hanteert. Het is aan de AIVD zorg te dragen voor de inhoudelijke kwaliteit van de gegevens, en de gegevens te actualiseren en te corrigeren. Het interne beleid van de AIVD dient te waarborgen dat de eigen nationale standaard voldoende invulling geeft aan het zorgvuldigheidsvereiste.

Op het moment van het schrijven van dit rapport wordt hiervoor een werkinstructie door de AIVD opgesteld m.b.t. gegevensuitwisseling van de AIVD binnen CTG. De CTIVD heeft enkele gevallen aangetroffen waarbij de gegevensverstrekking van de AIVD op onderdelen onzorgvuldig waren. Deze onzorgvuldigheden zijn inmiddels hersteld.

Met betrekking tot één specifieke vorm van de uitwisseling van *geëvalueerde* gegevens in het kader van sigint samenwerking is de zorgvuldigheid onvoldoende geborgd. Er zijn geen multilaterale afspraken die waarborgen dat de gegevens correct zijn weergegeven, voldoende inhoudelijk onderbouwd en actueel zijn. In de praktijk is de herkomst van de gegevens onvoldoende inzichtelijk.

In het kader van de sigint samenwerking is multilateraal vastgelegd hoe lang bepaalde uitgewisselde gegevens uiterlijk bewaard worden. De gestelde bewaartermijn voor de uitgewisselde ongeëvalueerde gegevens is korter dan de Wiv 2002 (en de Wiv 2017) vereist. Deze multilaterale afspraak vormt daarmee een aanvullende waarborg voor zorgvuldigheid. Ook zijn in het kader van de sigint samenwerking multilaterale afspraken gemaakt over de mogelijkheid van controle en toezicht. De CTIVD ziet dit eveneens als een belangrijk waarborg. In de praktijk is effectief toezicht om technische redenen nog niet goed mogelijk.

Betrouwbaarheid

Betrouwbaarheid is eveneens een kwaliteitsvereiste. Het heeft betrekking op de mate waarin sprake is van vastgestelde, geverifieerde persoonsgegevens en dit wordt vermeld of aangeduid. Ook ziet betrouwbaarheid op de werking van gegevensverwerkingsprocessen en op gegevensbescherming in dat verband.

De Wiv 2002 vereist dat verwerkte gegevens zijn voorzien van een aanduiding omtrent de mate van de betrouwbaarheid of een verwijzing naar de bron waaraan de gegevens zijn ontleend. Hierin wordt door de AIVD *niet* voorzien bij de verstrekking van gegevens. Dit is **onrechtmatig**. De CTIVD heeft geen indicaties dat de door de AIVD verstrekte gegevens daadwerkelijk onvoldoende betrouwbaar zijn.

Waar het gaat om de betrouwbaarheid van systemen voor gegevensuitwisseling, stelt de wet enkel dat voorzieningen moeten worden getroffen ter beveiliging van de gegevensverwerking tegen verlies of aantasting van gegevens en tegen onbevoegde gegevensverwerking. De AIVD draagt hier een verantwoordelijkheid als beheerder van de CTG database. De CTIVD is van oordeel dat de AIVD deze verantwoordelijkheid feitelijk voldoende heeft ingevuld.

Eindconclusie

Gelet op het zwaarwegende belang van de internationale bestrijding van het jihadisme en de noodzaak tot intensieve samenwerking daarbij, is de CTIVD van oordeel dat de huidige uitvoeringspraktijk van de AIVD op dit moment grotendeels nog binnen de kaders van de wettelijke vereisten blijft. Op twee punten is sprake van structurele onrechtmatigheid: het niet maken van een risicoweging aan de hand van de criteria die gelden voor de samenwerking met buitenlandse diensten en het niet voorzien in een aanduiding van de betrouwbaarheid van verstrekte gegevens. Op één punt is sprake van incidentele onrechtmatigheid: het gedurende vijf maanden ontbreken van toestemming voor de verstrekking van ongeëvalueerde gegevens.

Behoudens deze onrechtmatigheden, heeft de CTIVD geen door de AIVD verstrekte geëvalueerde of ongeëvalueerde gegevens aangetroffen die niet voldeden aan de vereisten van noodzakelijkheid, behoorlijkheid en zorgvuldigheid. Voor zover de AIVD een verantwoordelijkheid draagt voor de zorgvuldige en betrouwbare inrichting van systemen voor gegevensuitwisseling, heeft de AIVD dit

voldoende ingevuld. De multilaterale gegevensuitwisseling van de AIVD m.b.t. (vermeende) jihadisten is tot op heden in de praktijk **rechtmatig** te noemen.

Op een aantal punten zijn de waarborgen voor de bescherming van de grondrechten van de burger echter onvoldoende stevig verankerd. Binnen de CTG is beperkt sprake van gemeenschappelijk afspraken waarmee concreet wordt voorzien in adequate rechtsbescherming van het individu. In het kader van de sigint samenwerking is hier wel invulling aan gegeven maar zijn er redenen bestaande waarborgen te versterken of aan te vullen. De maatschappelijke en technische ontwikkelingen op het terrein van de aanpak van jihadisme zijn sterk in beweging. De CTIVD signaleert in die context dat op een aantal terreinen sprake is van risico's die, wanneer deze zich verwezenlijken, ook kunnen leiden tot onrechtmatig handelen door de AIVD. In het volgende hoofdstuk worden deze risico's geduid en worden daartoe aanbevelingen gedaan.

8 Risico's en aanbevelingen

8.1 Inleiding

In dit rapport gaat de CTIVD in de wijze waarop op dit moment invulling wordt gegeven aan de wettelijke vereisten van noodzakelijkheid, behoorlijkheid, zorgvuldigheid en (de aanduiding van) betrouwbaarheid bij de multilaterale gegevensuitwisseling van de AIVD met betrekking tot (vermeende) jihadisten (hoofdstuk 6 en bijlage II). Zij komt in hoofdstuk 7 tot de conclusie dat, mede gelet op het zwaarwegende belang van de internationale bestrijding van het jihadisme en de noodzaak tot intensieve samenwerking daarbij, de huidige uitvoeringspraktijk grotendeels blijft binnen de kaders van de genoemde vereisten.

De maatschappelijke en technische ontwikkelingen op dit terrein zijn echter sterk in beweging. Op een aantal punten zijn de waarborgen voor de bescherming van de grondrechten van de burger (nog) onvoldoende stevig verankerd. Om te voorkomen dat in deze dynamiek onrechtmatigheden ontstaan is de tegenwoordig in veel organisaties gebruikte risicobenadering toegepast. De CTIVD ziet hier risico's die al aan de orde zijn maar nog geen of beperkt effect hebben gehad en risico's die in de (nabije) toekomst aan de orde kunnen komen. In dit hoofdstuk gaat zij nader in op deze risico's en doet zij aanbevelingen om de (verdere) manifestatie hiervan te voorkomen.

De CTIVD bespreekt de door haar geconstateerde risico's vanuit het perspectief van de Wiv 2002 (en de Wiv 2017). Het is voor de rechtmatigheid van de multilaterale gegevensuitwisseling door de AIVD noodzakelijk dat wanneer de AIVD participeert in bepaalde samenwerkingsvormen het niveau van rechtsbescherming dat daarbij aan de orde is, niet lager ligt dan het niveau van rechtsbescherming dat wordt geboden door de Wiv 2002 (en de Wiv 2017). Dit betekent niet dat elk specifiek vereiste uit de Wiv 2002 (en de Wiv 2017) invulling moet krijgen in multilaterale afspraken. Het betekent wel dat voldoende waarborgen moeten bestaan voor de bescherming van het individu bij de uitwisseling en verdere verwerking van gegevens in het kader van de onderzochte multilaterale samenwerking.

8.2 Risico's m.b.t. de CTG database

De CTG database heeft veel operationele voordelen ten opzichte van andere, meer traditionele wijzen van gegevensuitwisseling. De gegevensuitwisseling is sneller en makkelijker. In een kort tijdsbestek kan een grote groep diensten bereikt worden. Gegevens zijn inzichtelijk bij elkaar gebracht en *real time* beschikbaar. Het gebruik van de gegevens in het eigen inlichtingenproces is eenvoudiger en directer. Deze en andere operationele voordelen brengen echter ook bepaalde risico's of verantwoordelijkheden met zich mee. De belangrijkste worden hieronder besproken.

8.2.1 Risico's m.b.t. de juridische grondslag

- De samenwerkende veiligheidsdiensten zijn *gezamenlijk* verantwoordelijk voor de CTG database. De gezamenlijke verantwoordelijkheid strekt zich uit tot de gegevens in de database, het beheer van de database en de gegevensbescherming die daarbij geboden moet worden. Dit noodzaakt heldere multilaterale afspraken en gemeenschappelijke standaarden voor gegevensbescherming.

Aanbeveling: De CTIVD beveelt de AIVD aan te streven naar de concrete invulling van een gemeenschappelijk kader voor gegevensbescherming m.b.t. de CTG database en een duidelijke instructie voor het beheer van de database, op basis van multilaterale afspraken.

8.2.2 Risico's voor noodzakelijkheid

- Het is van wezenlijk belang dat sprake is van een voldoende hoge drempel voor het inbrengen van gegevens in de database. Het risico doet zich voor dat in de database gegevens worden opgenomen van personen die daar niet in thuis horen. Het dient voor iedere gebruiker van de database voldoende helder te zijn op basis van welke criteria of in welke omstandigheden een persoon aan de database kan worden toegevoegd. Is dat niet het geval, dan dreigt de database voorbij te gaan aan het doel waarvoor het is gecreëerd. De noodzakelijkheidsdrempel is nu vooral afhankelijk van wat elke deelnemende dienst zelf als drempel hanteert.

Aanbeveling: De CTIVD beveelt de AIVD aan te streven naar een multilateraal afgesproken definiëring van de targets die opgenomen dienen te worden in de database en, daarop vooruitlopend, een voldoende afgebakende definiëring in ieder geval intern vast te leggen.

8.2.3 Risico's voor behoorlijkheid

- Naarmate in de database meer en gevoeliger gegevens worden gedeeld, ontstaat het risico dat de inmenging op grondrechten zwaarder wordt en op een zeker moment niet langer in verhouding staat tot het gewicht van de operationele belangen die met de verstrekking van de gegevens worden gediend. Dit risico is vooral aan de orde wanneer persoonsgegevens een gevoelig karakter hebben, bijvoorbeeld doordat zij gaan over iemands gezondheid, of betrekking hebben op een kwetsbare categorie personen, zoals minderjarigen. Het is noodzakelijk dat dergelijke persoonsgegevens in de database inzichtelijker worden gemaakt, zodat de verhouding tussen inmenging op grondrechten en operationele belangen bewaakt kan worden. Een voorbeeld daarvan is het verbinden van een onderscheidend kenmerk aan gegevens die betrekking hebben op minderjarigen. Daarmee wordt direct duidelijk gemaakt dat het gaat om gegevens waaraan meer gewicht moet worden gehangen in termen van inmenging op grondrechten.

Aanbeveling: De CTIVD beveelt de AIVD aan de gegevensuitwisseling m.b.t. minderjarigen en bijzondere categorieën persoonsgegevens in de database te voorzien van een specifiek kenmerk zodat direct duidelijk is dat het gaat om persoonsgegevens waarbij het gewicht van de inmenging in grondrechten zwaarder is. Ook beveelt zij de AIVD aan in intern beleid nader handvatten te bieden welke persoonsgegevens wel en niet in aanmerking komen voor verstrekking via de database.

8.2.4 Risico's voor zorgvuldigheid

- Zorgvuldigheid vereist het actueel houden van de database door het verwijderen van incorrecte of niet langer relevante gegevens en het toevoegen van nieuwe gegevens. De kwaliteit van de database in zijn geheel staat of valt met de mate waarin hier zorgvuldig mee om wordt gegaan. Dit is nu afhankelijk van nationale standaarden. Deze kunnen echter aanzienlijk van elkaar verschillen. Het inzichtelijk maken wanneer welk gegeven aan de database is toegevoegd, kan bijdragen aan duidelijkheid over de actualiteit van gegevens. De CTIVD constateert dat de CTG database in het najaar van 2017 door de AIVD is aangepast en nu hierin faciliteert. Gelet op de totale hoeveelheid persoonsgegevens in de database en de verwachting dat dit alleen maar zal toenemen de komende tijd, is het noodzakelijk aan te sturen op multilaterale afspraken over het actualiseren en verwijderen van gegevens. Zo zou gedacht kunnen worden aan een periodieke inhoudelijke kwaliteitscontrole en aan een maximum bewaartermijn van de multilateraal uitgewisselde gegevens.

- Ten tijde van het onderzoek was geen sprake van beleid van de AIVD hoe en door wie wordt voorzien in het actueel houden en zo nodig vernietigen van door de AIVD verstrekte gegevens in de database. Inmiddels is hier wel sprake van. In augustus 2017 heeft de AIVD beleid vastgesteld waarin dit is opgenomen.

Aanbeveling: De CTIVD beveelt de AIVD aan te streven naar multilaterale afspraken over een mechanisme voor het actueel houden van de gegevens in de database en het verwijderen van niet langer relevante gegevens. In dat kader zou ook kunnen worden voorzien in systeemtechnische waarborgen die garanderen dat wanneer gegevens een bepaalde tijd niet geactualiseerd noch bekeken zijn, de gegevens worden vernietigd.

- De AIVD heeft de mogelijkheid persoonsgegevens over te nemen die door een andere dienst zijn ingebracht en door die dienst vernietigd zullen worden. Deze mogelijkheid is niet nader ingekaderd. De CTIVD ziet hier een belangrijk risico voor de bescherming van de grondrechten van het individu. Indien nationale regelgeving een deelnemende dienst verplicht persoonsgegevens te vernietigen, bijvoorbeeld omdat deze onrechtmatig zijn verwerkt, mag het niet zo zijn dat deze gegevens zonder meer kunnen worden overgenomen door een andere dienst en alsdan in de CTG database blijven staan. Dan zou sprake zijn van het omzeilen van nationale waarborgen.

Aanbeveling: De CTIVD beveelt de AIVD aan, aan te sturen op een multilaterale regeling die het kunnen overnemen van persoonsgegevens beperkt tot die gevallen waarin de vernietiging van de persoonsgegevens niet wordt vereist door nationale wetgeving. Ook beveelt zij de AIVD aan intern te voorzien in een instructie voor het overnemen van persoonsgegevens die deze beperking waarborgt.

8.2.5 Risico's voor betrouwbaarheid

- Het risico bestaat dat persoonsgegevens met een beperkte betrouwbaarheid worden opgenomen in de database zonder dat dit kenbaar is en dat op basis van die gegevens wordt gehandeld.

- De AIVD heeft in augustus 2017 m.b.t. de eigen gegevensverstrekking intern beleid vastgesteld waarin is opgenomen dat alleen een bepaald type gegevens met een zeker niveau van betrouwbaarheid mag worden gedeeld via de database.

Aanbeveling: De CTIVD beveelt de AIVD aan, aan te sturen op multilaterale afspraken over standaarden voor c.q. een aanduiding van de betrouwbaarheid van persoonsgegevens in de CTG database.

- Voor de toegang tot het systeem van de database en de mogelijkheid gegevens toe te voegen, zijn door de AIVD als beheerder van het systeem geen specifieke beperkingen aangebracht.

Aanbeveling: De CTIVD beveelt de AIVD aan, aan te sturen op multilaterale afspraken over de kring van personen die toegang wordt verleend c.q. wordt geautoriseerd gegevens toe te voegen aan de database.

8.3 Risico's m.b.t. het operationeel platform van de CTG

8.3.1 Risico's voor zorgvuldigheid

- De CTIVD ziet risico's in het door de AIVD mondeling uitwisselen van gegevens binnen het operationeel platform. Bij het verstrekken van persoonsgegevens aan diensten die naar aanleiding daarvan maatregelen kunnen treffen, is het wettelijk vereist dat de verstrekking schriftelijk plaatsvindt. De reden hiervoor is vooral gelegen in het kunnen herleiden van de gegevens waarop maatregelen die rechtsgevolgen hebben voor de burger zijn gebaseerd. Het is de vraag of de verslaglegging die wordt gemaakt van de bijeenkomsten van het operationeel platform een toereikende waarborg vormt voor het vereiste dat persoonsgegevens schriftelijk worden verstrekt. De verslaglegging wordt pas na enige tijd vastgesteld en omvat een veelheid aan gegevens. Vanwege de mogelijkheid dat de gegevensuitwisseling leidt tot maatregelen tegen personen, is extra zorgvuldigheid vereist. Die zorgvuldigheid kan zijn gelegen in de afspraak dat naar aanleiding van de mondeling verstrekte persoonsgegevens geen maatregelen worden getroffen, tenzij sprake is van spoed. Een waarborg daartoe ontbreekt op dit moment.

- De CTIVD ziet bovendien een risico in de samenwerking door de AIVD buiten de bijeenkomsten van het platform om; in het permanent en dagelijks naast elkaar werken van de vertegenwoordigers van de deelnemende diensten. De permanente fysieke aanwezigheid werkt in de hand dat persoonsgegevens door de AIVD makkelijker mondeling met een of enkele diensten worden uitgewisseld. Hoewel bilaterale gegevensuitwisseling niet het onderwerp is van deze fase van het onderzoek, vindt de CTIVD het wel van belang dit risico hier te adresseren.

Aanbeveling: De CTIVD beveelt de AIVD aan, aan te sturen op multilaterale afspraken over beperkingen voor het mondeling verstrekken van persoonsgegevens binnen het operationeel platform, en hierover een instructie voor het eigen personeel op te stellen.

8.4 Risico's m.b.t. samenwerkingsvormen binnen de sigint samenwerking

De aanbevelingen die in deze paragraaf zijn opgenomen gelden ook voor de MIVD.

8.4.1 Risico's m.b.t. de grondslag voor een bepaalde samenwerkingsvorm

- De CTIVD ziet m.b.t. de voorwaarde dat in de samenwerking met buitenlandse diensten de eigen wet- en regelgeving moet worden gevolgd, een moeilijkheid ontstaan met de inwerkingtreding van de nieuwe Wiv 2017. De Wiv 2017 geeft een strikter kader voor onderzoeksopdrachtgerichte interceptie en de verdere verwerking van de geïntercepteerde gegevens dan nu aan de orde is bij de ongerichte interceptie onder de Wiv 2002.

Aanbeveling: De CTIVD beveelt de AIVD (en de MIVD) aan in kaart te brengen welke gevolgen de nieuwe Wiv 2017 meebrengt voor de mogelijkheden van de AIVD (en de MIVD) op het terrein van sigint blijvend samen te werken in een bepaalde vorm.

- Hoewel het van grote waarde is dat multilaterale afspraken zijn gemaakt over het kunnen uitoefenen van controle en toezicht, is effectief toezicht nu nog niet voldoende mogelijk. Voor een deel wordt dit naar verwachting in 2018 mogelijk gemaakt.

Aanbeveling: De CTIVD beveelt de AIVD (en de MIVD) aan, aan te sturen op multilaterale afspraken die voorzien in gezamenlijk toezicht op het gebruik van gegevens en die het toezicht (technisch) mogelijk maken.

8.4.2 Risico's voor zorgvuldigheid

- Voor één specifieke vorm van gegevensuitwisseling geldt dat de zorgvuldigheid van de gegevensuitwisseling onvoldoende geborgd is. Hoewel het gebruik van deze gegevens beperkt is, doet het risico zich voor dat dit uiteindelijk leidt tot een onrechtmatige uitoefening van bevoegdheden.

Aanbeveling: De CTIVD beveelt de AIVD (en de MIVD) aan, aan te sturen op multilaterale afspraken die waarborgen dat de juistheid van de gegevens wordt geborgd. Het gaat er hierbij om te borgen dat de gegevens inhoudelijk kloppen, actueel en relevant zijn en dat inzichtelijk is wat de herkomst van de gegevens is. Ook beveelt zij de AIVD (en de MIVD), vooruitlopend hierop, intern vast te leggen hoe en door wie hier invulling aan wordt gegeven.

Tijdelijk adres:
Frederikkazerne, gebouw 35
Van Alkemadelaan 786 | 2597 Den Haag
Postbus 90701 | 2509 LS Den Haag

T 070 315 58 20 | **F** 070 381 71 68
E info@ctivd.nl | www.ctivd.nl