Bijlage II

Bij het toezichtsrapport over 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

BIJLAGE II

**bij het toezichtsrapport over
de multilaterale gegevensuitwisseling door de AIVD
over (vermeende) jihadisten**

Bevindingen van de CTIVD m.b.t. waarborgen voor multilaterale gegevensuitwisseling

1 Inleiding

Waarborgen voor de multilaterale gegevensuitwisseling m.b.t. (vermeende) jihadisten kunnen 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. 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 in ieder geval 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.

Algemene beginselen van gegevensbescherming hebben doorgaans een vertaling gekregen in nationale wetgeving die de activiteiten van inlichtingen- en veiligheidsdiensten regardeert. Dit is ook in Nederland het geval. De Wiv 2002 (en de nieuwe Wiv 2017) kent verschillende bepalingen voor gegevensbescherming. In paragraaf 2 van deze bijlage legt de CTIVD uit wat de wettelijke vereisten van noodzakelijkheid, behoorlijkheid, zorgvuldigheid en (aanduiding van) betrouwbaarheid inhouden in de context van de multilaterale gegevensuitwisseling van de AIVD m.b.t. vermeende jihadisten.

In deze bijlage 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. Het is de CTIVD niet toegestaan in deze openbare bijlage uitgebreid in te gaan op de inhoud van multilaterale afspraken, vanwege het staatsgeheime karakter daarvan. In bijlage II bij het geheime toezichtsrapport wordt daar wel nader op ingegaan.

Ook heeft de CTIVD (steekproefsgewijs) getoetst of de AIVD het beleid in de praktijk nakomt. De bevindingen van de CTIVD zijn hieronder, in de paragrafen 3 en 4, weergegeven. 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. Dit bespreekt de CTIVD in hoofdstuk 8 van het toezichtsrapport.

2 De wettelijke vereisten in beeld

2.1 Noodzakelijkheid

Het verstrekken van gegevens aan een buitenlandse dienst moet op basis van artikel 12 lid 2 Wiv 2002/ artikel 18 lid 1 Wiv 2017 noodzakelijk zijn voor een bepaald legitiem doel. Concreet betekent dit dat de AIVD:

1. een vooraf omschreven doel moet hebben dat past binnen de wettelijke taken die aan de AIVD zijn opgedragen;
2. de redelijke verwachting heeft dat door het verstrekken van de gegevens aan de specifieke buitenlandse dienst dit doel wordt bereikt;
3. dit kan onderbouwen.

Een zelfde systematiek geldt ook voor het gebruiken van gegevens die zijn ontvangen en voor het (gezamenlijk) analyseren van gegevens. Elke vorm van gegevensverwerking moet noodzakelijk zijn voor een bepaald legitiem doel. Dit vormt een belangrijke waarborg voor de bescherming van de grondrechten van de persoon wiens gegevens worden verwerkt.

Multilateraal doel

Waar het gaat om het verstrekken van gegevens binnen een multilateraal samenwerkingsverband is telkens sprake van een vrij algemeen doel. Dit is inherent aan het multilateraal delen van gegevens, zeker wanneer sprake is van een grotere groep. De AIVD heeft de verwachting dat met het verstrekken van gegevens m.b.t. (vermeende) jihadisten aan de andere buitenlandse diensten binnen het samenwerkingsverband, wordt bijgedragen aan de internationale bestrijding van het jihadisme. Het doel daarbij is het verbeteren van de gemeenschappelijke informatiepositie, oftewel het completeren van het beeld dat bestaat van de dreiging die voortkomt uit het jihadisme zodat die dreiging kan worden tegengegaan. De noodzakelijkheidsafweging is vrijwel gelijk voor elk van de targets wiens persoonsgegevens door de AIVD worden verstrekt. Het multilaterale karakter van de gegevensuitwisseling maakt dat het zich niet goed kan toespitsen op een concreter doel.

Drempel

Het voorgaande roept de vraag op wat dan de waarde is van de noodzakelijkheidsafweging. Op welke wijze vormt dit een waarborg voor de bescherming van grondrechten? Hoewel deze afweging in de praktijk van multilaterale samenwerking slechts een algemene invulling kan krijgen, vormt het naar het oordeel van de CTIVD wel een *drempel* voor gegevensuitwisseling of –analyse. Die drempel wordt hoger naarmate specifieker wordt vastgelegd welke gegevensuitwisseling of -analyse voor dat doel noodzakelijk is. De drempel wordt lager naarmate dit algemener wordt omschreven of voor velerlei interpretatie vatbaar is.

Met andere woorden, de waarborg van noodzakelijkheid in multilaterale samenwerking vereist een heldere definiëring van de gevallen waarin tot gegevensuitwisseling kan worden overgegaan. Gaat het om personen die daadwerkelijk zijn uitgereisd, die een poging daartoe hebben ondernomen of die plannen daartoe hebben? Hoe zit het met vrouwen en kinderen die worden meegenomen? Betreft het ook personen die jihadstrijders rekruteren of uitreizen faciliteren, bijvoorbeeld door het financieren of het organiseren ervan? Welke drempel wordt gehanteerd voor het uitwisselen van persoonsgegevens binnen het samenwerkingsverband?

2.2 Behoorlijkheid

Behoorlijkheid houdt in dat het doel van de gegevensuitwisseling in verhouding staat tot de nadelen ervan voor de betrokken persoon. Het gaat hier met name om de inmenging in iemands grondrechten doordat gegevens worden verstrekt aan een groep buitenlandse diensten die deze gegevens kunnen gebruiken in hun eigen inlichtingenproces. Tegenover de inmenging die wordt gemaakt in iemands grondrechten moeten belangen staan die voldoende zwaar wegen. Dit betreft het doel dat door de AIVD wordt beoogd te bereiken. Wanneer het gewicht van de inmenging in grondrechten zwaarder weegt dan het gewicht van de operationele belangen daarbij, is sprake van onbehoorlijkheid.

Gewicht van de inmenging

Het gewicht van de inmenging in iemands grondrechten bij het multilateraal verstrekken van persoonsgegevens wordt bepaald door:

1. Het aantal buitenlandse diensten en/of andere instanties waaraan wordt verstrekt;

Hoe groter de kring van instanties die toegang heeft tot of de beschikking krijgt over de persoonsgegevens, hoe groter de inmenging in de grondrechten van de persoon wiens gegevens worden verstrekt. Niet alleen het direct verstrekken van gegevens speelt hier een rol, maar ook de mate van doorverstrekking van die gegevens aan derden. Hierover kunnen concrete multilaterale afspraken worden gemaakt. Of de AIVD ervan uit kan gaan dat zijn gegevens niet zonder meer verder worden verstrekt aan andere instanties, is vooral een kwestie van vertrouwen en ervaring opgedaan in de samenwerkingsrelatie. In de eerder genoemde risicoweging dient tot uiting te komen of op dit punt sprake is van risico's.

2. Het gebruik van de gegevens door die diensten en instanties;

Wanneer de verstrekking leidt of kan leiden tot het nemen van strafrechtelijke, bestuursrechtelijke of andere maatregelen tegen de persoon, dan legt dat meer gewicht in de schaal dan wanneer hier geen sprake van is. In dit kader is het van belang dat de AIVD goed in beeld heeft wat de aard en taken zijn van de dienst(en) waaraan de gegevens worden verstrekt. Bij een veiligheidsdienst met een opsporingstaak is het risico groter dat door de AIVD verstrekte gegevens worden gebruikt bij het nemen van maatregelen tegen een persoon, dan bij een veiligheidsdienst die geen gecombineerde taken heeft. Dergelijke risico's dienen te worden geadresseerd in de wegingsnotities die per buitenlandse dienst moeten worden opgesteld. Of de AIVD ervan uit kan gaan dat zijn gegevens niet worden gebruikt voor andere doeleinden of op andere wijzen dan is afgesproken, is ook een kwestie van vertrouwen en ervaring opgedaan in de samenwerkingsrelatie. In de eerder genoemde risicoweging dient tot uiting te komen of op dit punt sprake is van risico's.

3. De hoeveelheid persoonsgegevens en de gevoeligheid van de gegevens die worden verstrekt.

Het maakt verschil of alleen identificerende gegevens worden verstrekt, zoals een naam, geboortedatum of telefoonnummer, dan wel ook sprake is van de verstrekking van andere persoonlijke gegevens, zoals de gezinssituatie van de betrokken persoon en zijn activiteiten op sociale media. Het gewicht van de inmenging neemt toe naarmate sprake is van bijzonder gevoelige categorieën personen of persoonsgegevens. Hier kan gedacht worden aan gegevens m.b.t. minderjarigen of aan gegevens die verband houden met iemands gezondheid of seksuele leven. Dergelijke categorieën verdienen extra bescherming. In de Wiv 2002 zijn aanvullende waarborgen opgenomen m.b.t. bijzondere categorieën persoonsgegevens (artikel 13 lid 3 en 4). De verwerking van dergelijke gegevens mag alleen plaatsvinden in aanvulling op de verwerking van andere gegevens en voor zover dat onvermijdelijk is voor het te bereiken doel.

Gewicht van de (operationele) belangen

Het tegenwicht aan de andere kant van de weegschaal bestaat uit het doel dat men wil bereiken met de gegevensuitwisseling of –analyse. Zoals hierboven onder noodzakelijkheid is aangegeven, is dit doel in het geval van multilaterale samenwerking algemeen van aard en gelijk voor elke uitwisseling of analyse die plaatsvindt. Het gaat daarbij telkens om het versterken van de (gezamenlijke) informatiepositie ten behoeve van de internationale bestrijding van het jihadisme.

Dit doel krijgt meer of minder gewicht door de prioritering die aan het desbetreffende target gegeven wordt. Met prioritering wordt bedoeld hoe belangrijk de AIVD de persoon in kwestie vindt voor het onderzoek dat de dienst verricht. Deze prioritering kan in belangrijke mate worden vastgesteld aan de hand van de dreiging die uitgaat van een persoon, maar ook andere omstandigheden kunnen daarbij een rol spelen. Zo is de dreiging die uitgaat van iemand die is uitgereisd, gevechtservaring heeft opgedaan en terugkeert naar Europa doorgaans groter dan van iemand die enkel financiële ondersteuning biedt of jihadstrijders rekruteert. Wanneer een terugkeerder wordt aangehouden en in detentie wordt geplaatst, zijn de omstandigheden m.b.t. deze persoon zo dat hij een lagere prioritering behoeft dan een terugkeerder die zich nog vrijelijk kan bewegen. De prioritering bepaalt het tegenwicht voor de zwaarte van de inmenging op iemands grondrechten.

2.3 Zorgvuldigheid

Het zorgvuldigheidsvereiste is neergelegd in artikel 12 lid 3 Wiv 2002/artikel 18 lid 2 Wiv 2017 (gegevensverwerking) en artikel 16 sub a Wiv 2002 / artikel 24 lid 2 sub 2 Wiv 2017 (gegevens-verwerkingsprocessen).

Zorgvuldigheid m.b.t. verstrekte gegevens

Zorgvuldigheid heeft betrekking op de inhoudelijke juistheid van de persoonsgegevens die worden uitgewisseld en op de correcte weergave van die gegevens. De ontvanger van de persoonsgegevens moet ervan uit kunnen gaan dat de gegevens kloppen, dat wil zeggen gestaafd worden door onderliggende gegevens en correct zijn verwoord. Daarbij is het ook van belang dat de persoonsgegevens eenduidig zijn en niet op verschillende manieren geïnterpreteerd kunnen worden. Onderdeel van de juistheid van de gegevens is ook dat de gegevens voldoende actueel zijn, met name waar het gaat om uitgewisselde gegevens die zijn opgeslagen en door andere diensten geraadpleegd kunnen worden. De gebruiker moet ervan uit kunnen gaan dat de gegevens niet achterhaald zijn door andere gegevens van recentere datum.

Ook is het van belang hoe de gegevens worden verstrekt. De Wiv 2002 vereist dat persoonsgegevens schriftelijk worden verstrekt indien de ontvanger bevoegd is op basis van die gegevens maatregelen te treffen (artikel 40). Slechts in spoedeisende gevallen kan hiervan worden afgeweken. De vraag of een buitenlandse dienst die bevoegdheid heeft, dient beantwoord te worden in het kader van de hierboven genoemde risicoweging aan de hand van samenwerkingscriteria. Onderdeel hiervan is het in kaart brengen van de wettelijke bevoegdheden van de desbetreffende buitenlandse dienst. Bij het ontbreken van een dergelijke weging dient de AIVD naar het oordeel van de CTIVD ervan uit te gaan dat de buitenlandse dienst inderdaad bevoegd is maatregelen te treffen. Schriftelijke verstrekking van persoonsgegevens is daarmee een basisvoorwaarde. Als de persoonsgegevens in een spoedsituatie toch mondeling worden verstrekt, moet dit in ieder geval schriftelijk worden vastgelegd (artikel 42).

Een ander onderdeel van zorgvuldigheid betreft de vernietiging van gegevens. De AIVD dient periodiek te toetsen of door de dienst verstrekte gegevens die door andere diensten raadpleegbaar zijn (nog) betekenis hebben voor het doel waarvoor zij worden verwerkt. Is dat niet het geval, dan moeten de gegevens worden verwijderd (artikel 43 lid 1 Wiv 2002). Ook gegevens die onjuist zijn of ten onrechte zijn verstrekt, moeten worden verwijderd (artikel 43 lid 2 Wiv 2002).

Zorgvuldigheid m.b.t. het systeem

Zorgvuldigheid ziet ook op (geautomatiseerde) gegevensverwerkingsprocessen. In de Wiv 2002 is daartoe neergelegd dat de nodige voorzieningen moeten worden getroffen ter bevordering van de juistheid en de volledigheid van de gegevens die worden verwerkt (artikel 16 sub a). Dit houdt ook in dat het systeem moet voorzien in de vernietiging van gegevens. In de Wiv 2017, die nog niet in werking is getreden, is een meer omvattende zorgplicht voor de kwaliteit van gegevensverwerking opgenomen (artikel 24 lid 2 sub a).

2.4 Betrouwbaarheid

Aanduiding van betrouwbaarheid van persoonsgegevens

Betrouwbaarheid heeft betrekking op de mate waarin sprake is van vastgestelde, geverifieerde persoonsgegevens. Hierbij is van belang wie of wat de bron is van de gegevens, of die bron betrouwbaar is en wat de waarschijnlijkheid is dat de gegevens waar zijn. In artikel 12 lid 4 Wiv 2002 staat dat door de AIVD verwerkte gegevens moeten zijn voorzien van een aanduiding omtrent de mate van de betrouwbaarheid of een verwijzing naar de bron waaraan de gegevens zijn ontleend.

De betrouwbaarheid van gegevens die zijn verstrekt, is voor een andere dienst moeilijk te achterhalen. Het is in belangrijke mate een kwestie van vertrouwen en ligt in het verlengde van de inschatting van de professionaliteit en betrouwbaarheid van de buitenlandse dient zelf. Het betreft hier een van de samenwerkingscriteria aan de hand waarvan de hierboven besproken risicoweging plaatsvindt. Zonder risicoweging is het niet inzichtelijk of en in welke mate sprake is van risico's op dit vlak.

Betrouwbaarheid van het systeem

Betrouwbaarheid ziet ook op (geautomatiseerde) gegevensverwerkingsprocessen, bijvoorbeeld een systeem voor gegevensuitwisseling. Zijn de gegevens voldoende beschermd? Kunnen gegevens niet zonder meer door een ieder aangepast, verwijderd of vernietigd worden? Is de toegang tot de gegevens voldoende beperkt? In de wet is vastgelegd dat het hoofd van de dienst zorg moet dragen voor de nodige voorzieningen van technische en organisatorische aard ter beveiliging van de gegevensverwerking tegen verlies of aantasting van gegevens en tegen onbevoegde gegevensverwerking (artikel 16 sub b). Deze bepaling is ook in de Wiv 2017 opgenomen (artikel 24 lid 2 sub a).

3 Waarborgen voor gegevensuitwisseling door de AIVD binnen de CTG

3.1 Noodzakelijkheid gegevensuitwisseling

Voor zover geen sprake is van een duidelijke multilaterale definiëring van de gevallen waarin gegevensuitwisseling via de CTG database noodzakelijk wordt geacht, dient de AIVD een eigen drempel te hanteren. De CTIVD constateert dat de AIVD tot begin 2017 alleen persoonsgegevens verstrekte binnen de CTG indien het een persoon betrof die daadwerkelijk is uitgereisd of waarvan aanwijzingen bestaan dat deze concrete betrokkenheid heeft bij aanslagplanning. Hierin is begin 2017 verandering gekomen. Sinds enige tijd worden ook gegevens in de database geplaatst m.b.t. personen die niet zijn uitgereisd en personen waarvan een minder grote dreiging uitgaat. Van sommige personen in de database wordt niet vermeld welke terroristische activiteiten opname in de database noodzakelijk maken. De CTIVD stelt vast dat het wel telkens gaat om personen waarnaar de AIVD actief onderzoek verricht.

De AIVD heeft in augustus 2017 vastgelegd in intern beleid in welke gevallen wel en niet tot verstrekking kan worden overgegaan. In het beleid is opgenomen dat het moet gaan om “geduide contra terrorisme targets” en dat het “voor de taakuitvoering noodzakelijk moet zijn om gegevens m.b.t. deze targets te delen met alle CTG-partners”. De CTIVD vindt dat deze definiëring weinig toevoegt. Het is dermate algemeen dat het de kring van personen over wie gegevens worden gedeeld niet kleiner maakt, in tegendeel. Het vormt een weinig betekenisvolle drempel voor gegevensuitwisseling via de CTG database.

Binnen het operationeel platform wordt per casus bepaald op welke kring van personen het onderzoek zich kan richten. Tot dusver wordt gewerkt met een voldoende duidelijke afbakening van een dergelijke groep personen. De persoonsgegevens die door de AIVD worden verstrekt, vallen binnen die afbakening.

3.2 Behoorlijkheid gegevensuitwisseling CTG

Gewicht van de inmenging

Bij de CTG gaat het doorgaans om verstrekking van gegevens aan 29 diensten. Elk gegeven dat in de database wordt toegevoegd is (vrijwel) direct beschikbaar voor alle deelnemende diensten. Voor de gegevens die in het operationeel platform worden gedeeld geldt doorgaans een beperktere kring van deelnemende dienst, afhankelijk van wie deelnemen. Deelname staat open voor alle 30 diensten.

De gegevens mogen niet verder verstrekt worden. Deze regel, die ook wel de derde partijregel wordt genoemd, is voor de AIVD vastgelegd in de wet (artikel 37 Wiv 2002/artikel 65 Wiv 2017). Bij elke verstrekking door de AIVD wordt in de database aangegeven of de AIVD met betrekking tot de persoonsgegevens toestemming geeft voor de doorverstrekking aan nationale instanties werkzaam op het terrein van terrorismebestrijding.

De CTIVD stelt vast dat gegevens die door de AIVD binnen de CTG zijn verstrekt, bedoeld zijn voor gebruik in het inlichtingenproces van de deelnemende diensten. Gebruik buiten het inlichtingenproces, bijvoorbeeld ten behoeve van het strafproces, is alleen toegestaan indien de derde partijregel wordt gevolgd (zoals hierboven geschetst). Gebruik buiten het doel van de internationale bestrijding van het jihadisme is niet toegestaan.

De verstrekking van gegevens door de AIVD via de CTG database leidt niet automatisch tot het treffen van maatregelen, zoals bevriezing van iemands financiële middelen. Daarvoor gelden andere nationale en internationale procedures, die losstaan van de gegevensuitwisseling binnen de CTG. Wel kan aan de hand van de verstrekte gegevens signalering plaatsvinden in nationale of internationale signaleringssystemen, zoals het Schengen Informatie Systeem (SIS). Signalering maakt controle aan de grens mogelijk.

Het is de CTIVD in haar onderzoek gebleken dat het vooralsnog gaat om het uitwisselen door de AIVD van identificerende gegevens en in beperkte mate om andere persoonlijke gegevens. Het is aan de AIVD zelf een afweging te maken welke gegevens over een target wel en niet via de database worden verstrekt. Het plaatsen door de AIVD van een grote hoeveelheid en diversiteit aan gegevens per target is mogelijk maar nog niet aan de orde geweest. De CTIVD ziet hier een risico, naarmate meer en gevoeliger gegevens worden gedeeld. Zij bespreekt dit in hoofdstuk 8. Binnen het operationeel platform deelt de AIVD eveneens voornamelijk identificerende gegevens en in mindere mate andere persoonlijk gegevens.

De CTIVD heeft vooralsnog geen door de AIVD verstrekte gevoelige categorieën persoonsgegevens zoals bedoeld in artikel 13 lid 3 Wiv 2002 in de database aangetroffen. Evenmin heeft zij geconstateerd dat dergelijke gegevens door de AIVD zijn gedeeld in het operationeel platform. Het multilateraal verstrekken van gevoelige persoonsgegevens zal niet snel onvermijdelijk zijn voor het multilaterale doel van de verstrekking.

Het uitwisselen van gegevens van minderjarigen vindt wel plaats. De AIVD hanteert het beleid om persoonsgegevens te verstrekken met betrekking tot uitgereisde minderjarigen vanaf de leeftijd van 9 jaar. Vanaf die leeftijd kunnen minderjarigen volgens de AIVD ingezet worden als jihadstrijder.[1] De CTIVD signaleert een risico met betrekking tot de kenbaarheid van deze categorie personen in de CTG database. Zij bespreekt dit in hoofdstuk 8 van het toezichtsrapport.

Gewicht van de (operationele) belangen

Bij elke persoon die door de AIVD in de database is geplaatst, wordt een prioritering aangegeven. De AIVD hanteert daarvoor een prioriteringssystematiek. 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 dat de AIVD vanaf begin 2017 relatief meer lager geprioriteerde targets toevoegt aan de database.

De prioritering van een specifiek target wordt binnen het operationeel platform gezamenlijk bepaald door de deelnemende diensten. Waar de AIVD gegevens verstrekt binnen het operationeel platform, gaat het om targets die binnen de AIVD hoog tot middelhoog worden geprioriteerd.

3.3 Zorgvuldigheid gegevensuitwisseling CTG

Correcte weergave

Elk target dat door de AIVD in de database is opgenomen, is als zodanig kenbaar. Ook wanneer de AIVD gegevens toevoegt of aanvult op gegevens die door een andere dienst zijn ingebracht, is de herkomst van de gegevens kenbaar. De CTIVD heeft steekproefsgewijs onderzocht of gegevens die door de AIVD in de database zijn gezet, correct zijn weergegeven. Dit is het geval. Er zijn op dit punt slechts enkele kleine foutjes aangetroffen in de gegevens die zijn onderzocht. Deze zijn inmiddels door de AIVD hersteld.

---

[1] Zie ook de gezamenlijke publicatie van de NCTV en de AIVD “Minderjarigen bij ISIS”, 6 april 2017, beschikbaar op www.aivd.nl.

Voorzieningen ter bevordering van de correcte weergave

Voor de correcte weergave van persoonsgegevens in de CTG database zijn door de AIVD enkele systeemtechnische waarborgen gecreëerd. Zo is er een vast aantal velden dat per target moet worden ingevuld en een vast aantal velden dat kan worden ingevuld. Ook zijn er velden die volgens een vast format, dat wil zeggen telkens op dezelfde wijze, moeten worden ingevuld. De formats zijn niet dwingend. Afwijkingen worden door het systeem in het rood weergegeven. Daarnaast is een systematiek bedacht voor het geautomatiseerd onderkennen van foutief ingevoerde gegevens, dat wil zeggen gegevens die niet voldoen aan het format dat daarvoor is afgesproken. Indien hier sprake van is, wordt de verstrekkende dienst door het systeem geattendeerd op de incorrecte weergave van de gegevens en wordt een voorstel tot wijziging gedaan. De CTIVD constateert verder dat de database gebruiksvriendelijk is ingericht en goed doorzoekbaar is. De in te vullen velden zijn duidelijk en zijn voorzien van een informatie-icoon waarachter nadere uitleg te vinden is. Ook is sprake van een heldere gebruikershandleiding en worden door de AIVD trainingen verzorgd, zowel intern als aan andere diensten binnen de CTG. Het voorgaande draagt in belangrijke mate bij aan de correcte weergave van de gegevens in de database.

Juistheid en volledigheid

Bij de juistheid van de persoonsgegevens gaat het erom dat deze inhoudelijk correct en actueel zijn. Dit is niet alleen van belang bij het inbrengen van een nieuw target in de database. Wanneer in het onderzoek naar de activiteiten van een persoon nieuwe gegevens beschikbaar komen, is het aan de dienst die de gegevens initieel heeft verstrekt deze gegevens te wijzigen of aan te vullen. Dat dit gebeurt is van essentieel belang. De deelnemende CTG-diensten moeten er immers vanuit kunnen gaan dat de persoonsgegevens in de database correct en actueel zijn.

Er is veel gelegen aan de standaard die wordt gehanteerd door de dienst die de gegevens heeft verstrekt, zowel voor het inbrengen van de gegevens met betrekking tot een persoon als voor het telkens actualiseren daarvan. De nationale werkwijze van de AIVD moet dus in voldoende mate de juistheid van de gegevens waarborgen. Dit houdt in dat de gegevens in ieder geval (nog) inhoudelijk correct en actueel moeten zijn. Zo is het bijvoorbeeld van belang dat wanneer blijkt dat een persoon zich heeft gelieerd aan een andere strijdgroep, zich naar een ander land heeft verplaatst of is overleden, dit wordt aangepast in de database.

Binnen de AIVD geldt dat een teamhoofd toestemming moet geven voor het inbrengen van een nieuw target in de database. Daarnaast worden alle nieuw ingebrachte targets bekeken door een team dat zich specifiek richt op prioritering. Hier is sprake van een extra check. Het wijzigen of aanvullen van gegevens gebeurt door een bewerker. Hiervoor geldt een vier ogen principe: een senior bewerker kijkt mee. De werkwijze wordt op het moment van schrijven nader uitgewerkt in een interne werkinstructie.

De CTIVD heeft steekproefsgewijs onderzocht of gegevens die door de AIVD in de database zijn gezet correct en actueel zijn. Bij het merendeel van de gegevens is dit het geval. De CTIVD heeft echter ook enkele gegevens in de database aangetroffen die onvoldoende overeenkomen met de gegevens in de nationale systemen van de AIVD, bijvoorbeeld doordat deze onvolledig of nog niet geactualiseerd zijn. In hoofdstuk 8 van het toezichtsrapport wordt hier nader op ingegaan.

Voorzieningen ter bevordering van de juistheid

De AIVD heeft voorzien in mechanismen die bijdragen aan het onderkennen van onjuiste gegevens. Hier van belang is allereerst de mogelijkheid dat andere diensten gegevens toevoegen aan de gegevens die met betrekking tot een bepaalde persoon in de database zijn geplaatst. Op deze wijze kan een zekere kwaliteitsverbetering plaatsvinden. Sinds het najaar van 2017 is het in de database ook inzichtelijk wanneer gegevens het laatst zijn gewijzigd en door welke dienst. Dit kan een indicatie geven dat gegevens mogelijk niet meer actueel zijn.

Schriftelijke verstrekking

De basisvoorwaarde van schriftelijke verstrekking speelt met name een rol in het kader van het operationeel platform van de CTG. Dit platform is zo ingericht dat de vertegenwoordigers van de deelnemende diensten fysiek bij elkaar zitten op één locatie. Periodiek worden bijeenkomsten gehouden waar m.b.t. een bepaalde casus gegevens worden uitgewisseld. Het gaat hierbij om de uitwisseling van persoonsgegevens. De CTIVD constateert dat de AIVD van deze bijeenkomsten verslagen maakt. In deze verslagen wordt vastgelegd wie welke gegevens heeft verstrekt tijdens de platform bijeenkomst. De verslagen geven de indruk uitgebreid en gedetailleerd te zijn. De CTIVD ziet m.b.t. het mondeling verstrekken van persoonsgegevens wel bepaalde risico's. Zij gaat hier in hoofdstuk 8 van het toezichtsrapport verder op in.

Vernietiging van gegevens

De door de AIVD verstrekte gegevens in de database worden afhankelijk van het nationale regime bewaard. De AIVD beoordeelt zelf of de door de dienst verstrekte gegevens nog relevant zijn of vernietigd moeten worden. 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.

De database biedt geen systeemtechnische waarborgen voor vernietiging. Hier kan gedacht worden aan een alertering wanneer persoonsgegevens een bepaalde tijd niet zijn aangevuld of gewijzigd en wellicht niet meer relevant zijn. Ook kan worden gedacht aan automatische vernietiging na verloop van tijd.

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 ingeperkt.

Gegevens die binnen het operationeel platform zijn uitgewisseld behoren opgenomen te zijn in de verslagen van de bijeenkomsten van het platform. De verslagen worden verstrekt aan de diensten die hebben deelgenomen aan de desbetreffende bijeenkomsten. De AIVD dient m.b.t. de verslagen waarover de dienst beschikking heeft periodiek te toetsen of deze nog betekenis hebben voor het doel waarvoor ze zijn verwerkt.

Ook op het punt van vernietiging ziet de CTIVD risico's waar zij in hoofdstuk 8 van het toezichtsrapport nader op in gaat.

3.4 Betrouwbaarheid gegevensuitwisseling CTG

Aanduiding van betrouwbaarheid

Over het algemeen geldt dat inlichtingen- en veiligheidsdiensten hun bronnen geheim houden. Het inzicht geven in de precieze herkomst van de gegevens is op zijn minst ongebruikelijk. De samenwerking in het operationeel platform brengt hier enige verandering in. Het fysiek bij elkaar zitten en het intensief bespreken van concrete operationele casussen leidt ertoe dat de deelnemende diensten meer en meer inzicht geven in hun werkwijzen en bronnen van informatie. De betrouwbaarheid van gegevens kan in dat verband mondeling worden besproken.

De AIVD heeft in de CTG database voorzien in de mogelijkheid onzekere gegevens een rood kenmerk te geven. Dit impliceert dat de gegevens die geen rood kenmerk hebben, betrouwbare gegevens zijn. Wat precies als vastgestelde of geverifieerde gegevens geldt, kan verschillen per deelnemende dienst.

Voor de gegevens die de AIVD heeft verstrekt, is wettelijk vereist dat deze zijn voorzien van een betrouwbaarheidsindicatie of een bronverwijzing. Hierin wordt niet voorzien. Evenmin is intern vastgelegd dat de AIVD alleen volledig betrouwbare gegevens verstrekt via de database of binnen het operationeel platform. In augustus 2017 is wel in intern beleid van de AIVD opgenomen welk type gegevens mag worden verstrekt via de CTG database.

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.

Betrouwbaarheid van het systeem

De werking van de database op het gebied van de beveiliging van de gegevens is intern getoetst door de AIVD. Hierbij zijn een aantal aspecten van het systeem beoordeeld en is ingegaan op risico's, verantwoordelijkheden en beveiligingsmaatregelen. Dit leidde tot de conclusie dat het systeem geschikt wordt geacht voor het verwerken van gegevens tot het rubriceringsniveau geheim. De resultaten van de verrichte accreditatie zijn verstrekt aan alle diensten die deelnemen aan het samenwerkingsverband. De CTIVD heeft geen aanleiding te twijfelen aan de gedegenheid van dit accreditatieproces door de AIVD.
Een ander onderdeel van de accreditatie van het systeem betrof de toegang tot het systeem en de autorisatie om gegevens toe te voegen, te wijzigen of te vernietigen. De toegang tot het systeem is mogelijk gemaakt voor een grote groep deelnemers. De AIVD bepaalt voor de eigen dienst welke personen toegang dienen te hebben. Binnen de AIVD hebben in ieder geval alle medewerkers werkzaam op het contra terrorisme terrein toegang tot de database. Bewerkers van de contra terrorisme teams en enkele anderen zijn geautoriseerd gegevens toe te voegen en te wijzigen.

Waar het gaat om het wijzigen of vernietigen van gegevens, geldt overigens wel dat dit systeemtechnisch is voorbehouden aan de dienst die de gegevens initieel heeft verstrekt. Een andere deelnemende dienst kan dus geen gegevens wijzigingen of vernietigen die door de AIVD zijn ingebracht. Een uitzondering daarop is de dienst die de verantwoordelijkheid draagt over het functioneren van het systeem. Voor de AIVD is het als beheerder feitelijk mogelijk gegevens te wijzigen of te vernietigen.

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

4.1 Noodzakelijkheid gegevensuitwisseling sigint samenwerking

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 (zoals dat binnen de CTG plaatsvindt). Multilaterale afspraken binnen de sigint samenwerking geven invulling aan het noodzakelijkheidsvereiste. De drempel voor de uitwisseling van *ongeëvalueerde* gegevens ligt voldoende hoog. Ditzelfde geldt voor de uitwisseling van *geëvalueerde* gegevens.

4.2 Behoorlijkheid gegevensuitwisseling sigint samenwerking

Gewicht van de inmenging

Het gewicht van de inmenging in grondrechten wordt bepaald door het aantal diensten waaraan persoonsgegevens worden verstrekt, het gebruik van de gegevens en de hoeveelheid en gevoeligheid van de gegevens. Waar het gaat om het uitwisselen en analyseren van metadata (in bulk), heeft de waarborg van behoorlijkheid beperkte betekenis. Het is op voorhand immers niet duidelijk wiens persoonsgegevens worden verstrekt. De inmenging in grondrechten kan slechts in algemene zin en niet specifiek voor een concrete persoon in kaart worden gebracht.

Over het aantal diensten waaraan binnen de sigint samenwerking persoonsgegevens worden verstrekt, kan in het openbaar niets worden aangegeven. Het gaat in ieder geval om een kleiner aantal dan binnen de CTG aan de orde is.

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

Gewicht van de (operationele) belangen

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 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.

Op dit punt vormt de vereiste toestemming van de minister voor het uitwisselen van ongeëvalueerde gegevens een aanvullende waarborg. Juist omdat de behoorlijkheidsafweging niet goed te maken is , moet de minister afwegen 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 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. De CTIVD deed de aanbeveling de toestemming van de minister met betrekking tot het uitwisselen van ongeëvalueerde gegevens te beperken tot een jaar.[2] De minister van BZK nam deze aanbeveling over in een brief aan de Tweede Kamer van 30 juni 2016.[3]

Voor de sigint samenwerking op het terrein van de bestrijding van jihadisme is in juni 2014 toestemming gevraagd en verkregen. Daarna is op 6 december 2016 opnieuw toestemming van de minister verkregen voor de verstrekking van de ongeëvalueerde gegevens, op basis van een gemotiveerd verzoek daartoe. De AIVD heeft aangegeven dat de minister in de tussenliggende periode goed en volledig was geïnformeerd over de samenwerking. In juni 2016 heeft hij toestemming gegeven voor het ondertekenen van de MoU, wat volgens de AIVD impliciet ook betekent dat de minister toestemming gaf voor het uitwisselen van de ongeëvalueerde gegevens.

De CTIVD kan zich slechts ten dele vinden in dit argument. De verleende toestemming ziet niet specifiek op de verstrekking van ongeëvalueerde gegevens ten behoeve van contraterrorisme onderzoek. Gelet op het belang van de waarborg van ministeriële toestemming en de toezeggingen van de minister hierover, had ook tussen 30 juni 2016 en 6 december 2016 sprake moeten zijn van ministeriële toestemming voor het verstrekken van de ongeëvalueerde gegevens.

4.3 Zorgvuldigheid gegevensuitwisseling sigint samenwerking

Aan het zorgvuldigheidsvereiste wordt bij de uitwisseling van ongeëvalueerde gegevens voldoende invulling gegeven. De herkomst van de gegevens en de vernietiging daarvan zijn voldoende geborgd. Ook geldt als uitgangspunt dat gegevens schriftelijke verstrekt worden.

Met betrekking tot één specifieke vorm van de uitwisseling van *geëvalueerde* gegevens zijn er 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 deze gegevens onvoldoende inzichtelijk.

Correcte weergave

Bij de verstrekking van ongeëvalueerde gegevens speelt het zorgvuldigheidsvereiste een beperktere rol. Het betreft ruwe gegevens die niet nader bewerkt zijn. De data wordt kort nadat het is verzameld door de AIVD verstrekt. Dit gebeurt vrijwel geheel geautomatiseerd. Van een controle met betrekking tot de correcte weergave van elk persoonsgegeven kan gezien de hoeveelheid gegevens en het ongeëvalueerde karakter ervan geen sprake zijn.

Juistheid

In het kader van de sigint samenwerking zijn gezamenlijke afspraken gemaakt over de mogelijkheid van controle en toezicht op de zorgvuldige verwerking van gegevens. Het bestaan van deze multilaterale afspraken acht de CTIVD in de beoordeling van zorgvuldigheid van wezenlijk belang. In de praktijk is effectief toezicht vanwege technische redenen echter nog niet volledig mogelijk. De verwachting bestaat dat dit in 2018 wel het geval is.

---

[2] Zie in dit verband 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.

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

Schriftelijke verstrekking

Multilaterale afspraken waarborgen dat sprake is van schriftelijke verstrekking van persoonsgegevens.

Vernietiging van gegevens

In het kader van de sigint samenwerking is multilateraal afgesproken en vastgelegd hoe lang de verstrekte gegevens kunnen worden bewaard. De gestelde termijn past binnen de kaders die de Wiv 2002 (en de nieuwe Wiv 2017) daarvoor stelt.

Het is voor de CTIVD nog niet goed mogelijk te controleren of gegevens afkomstig van de AIVD na de afgesproken periode inderdaad vernietigd zijn. De CTIVD bespreekt dit in hoofdstuk 8.

4.4 Betrouwbaarheid gegevensuitwisseling sigint samenwerking

Aanduiding van betrouwbaarheid

Met betrekking tot de uitwisseling en analyse van gegevens binnen de sigint samenwerking geldt dat de betrouwbaarheid van de uitgewisselde gegevens vaststaat voor zover daarbij sprake is van een technische bron van gegevens.

Dit is anders bij gegevens die uit andere bron zijn verkregen. Op basis van artikel 12 lid 4 Wiv 2002 moeten verwerkte gegevens zijn voorzien van een betrouwbaarheidsindicatie of een verwijzing naar het document of de bron waaraan ze zijn ontleend. Dat is in de praktijk niet het geval. De AIVD voldoet niet aan dit vereiste, dat overigens ook in de nieuwe Wiv 2017 is opgenomen.

Betrouwbaarheid van het systeem

De CTIVD heeft geen aanwijzingen dat multilaterale systemen voor gegevensverwerking onvoldoende betrouwbaar zijn.

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