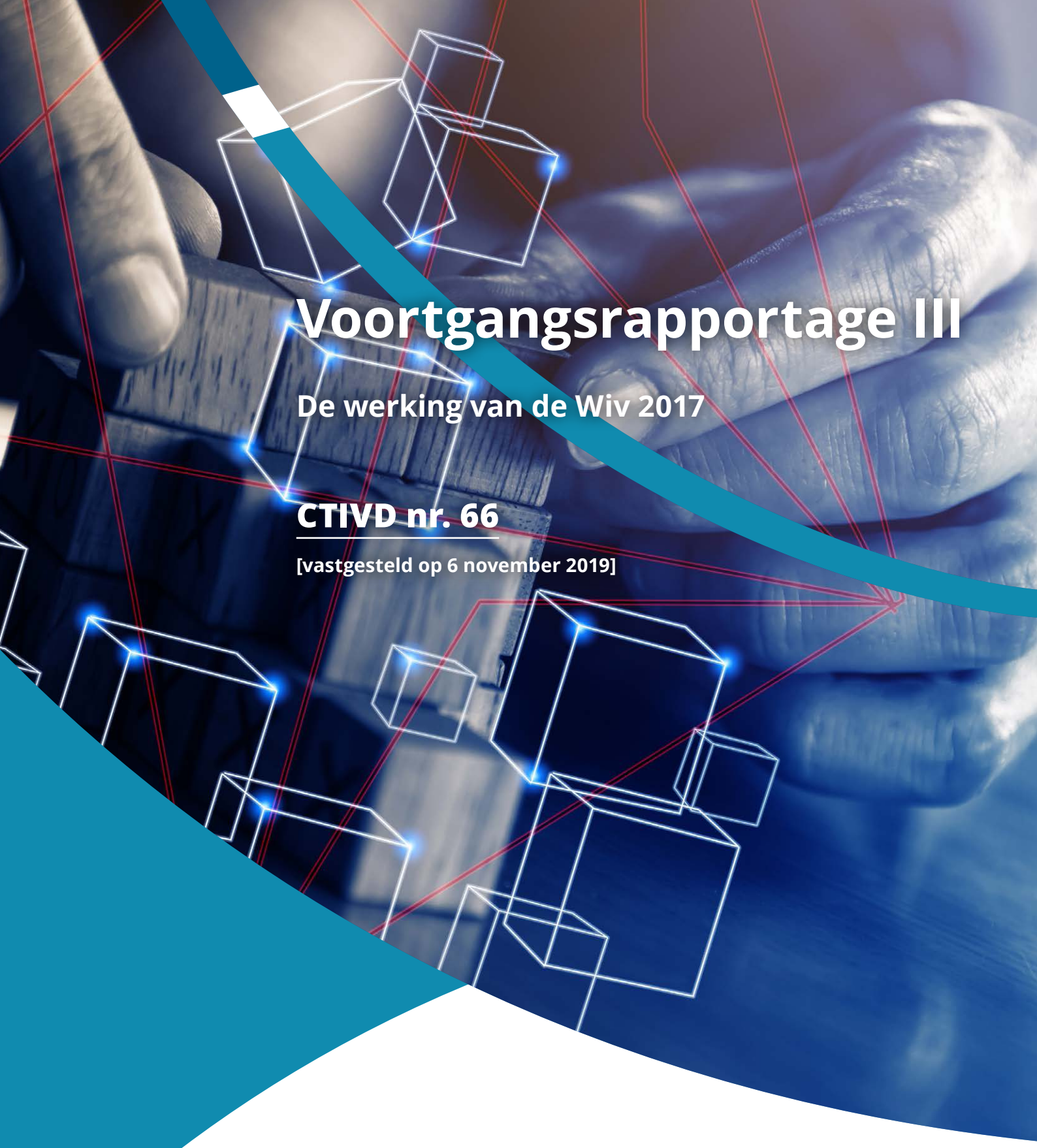

# Voortgangsrapportage III

## De werking van de Wiv 2017

**CTIVD nr. 66**

[vastgesteld op 6 november 2019]

Commissie van Toezicht
op de Inlichtingen- en
Veiligheidsdiensten

Commissie van Toezicht
op de Inlichtingen- en
Veiligheidsdiensten

**CTIVD nr. 66**

# VOORTGANGSRAPPORTAGE III

De werking van de Wiv 2017

## Inhoudsopgave


| | | | |
|---|---|---|---|
| **1** | **Inleiding** | | **3** |
| **2** | **Voortgang bij de diensten** | | **6** |
| | 2.1 | Algemeen beeld | 6 |
| | 2.2 | Voortgang m.b.t. de zorgplicht | 7 |
| | 2.3 | Voortgang m.b.t. datareductie | 8 |
| | 2.4 | Voortgang m.b.t. onderzoeksopdrachtgerichte interceptie | 11 |
| | 2.5 | Voortgang m.b.t. geautomatiseerde data-analyse | 13 |
| | 2.6 | Voortgang m.b.t. internationale samenwerking | 14 |
| **3** | **Informatiehuishouding en IT-omgeving diensten** | | **16** |
| | 3.1 | Inleiding | 16 |
| | 3.2 | Steekproef datareductie | 16 |
| | 3.3 | Steekproef geautomatiseerde data-analyse | 18 |
| **4** | **Vervolg** | | **21** |

Commissie van Toezicht
op de Inlichtingen- en
Veiligheidsdiensten

**CTIVD nr. 66**

# VOORTGANGSRAPPORTAGE III

**De werking van de Wiv 2017**

## 1 Inleiding

### Achtergrond

Op 1 mei 2018 is de nieuwe Wet op de inlichtingen- en veiligheidsdiensten 2017 (Wiv 2017) in werking getreden. Deze wet heeft in de afgelopen jaren veel politieke en maatschappelijke discussie teweeg gebracht. Centraal in dat debat staat de vraag of de vergaande noodzakelijke bevoegdheden van de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) en de Militaire Inlichtingen- en Veiligheidsdienst (MIVD) ter bescherming van de nationale veiligheid in balans zijn met de waarborgen voor de rechtsbescherming van de burger, zoals het recht op privacy en de algemene beginselen voor de bescherming en verwerking van persoonsgegevens. De Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (CTIVD) ziet het als haar kerntaak blijvend inzicht te geven in die balans. Zij heeft haar toezichtsactiviteiten vanaf 1 mei 2018 mede op nadrukkelijk verzoek van het parlement en het kabinet[1] gericht op de invoering van de nieuwe wet, in het bijzonder met betrekking tot de thema's die in het politiek en maatschappelijk debat veel aandacht hebben gekregen.

### Voortgangsrapportage I

In december 2018 publiceerde de CTIVD haar eerste voortgangsrapportage over de invoering van de Wiv 2017. Het algemeen beeld dat daaruit naar voren kwam, was dat de AIVD en de MIVD nog fundamentele stappen moesten zetten bij de invoering van essentiële onderdelen van de nieuwe wet. Er was sprake van een achterstand en op onderdelen hoge risico's voor onrechtmatig handelen bij beide diensten. Essentiële waarborgen voor de rechtsbescherming van de burger misten nog, geheel of gedeeltelijk, hun invulling in intern beleid, werkprocessen en de inrichting van technische systemen. Instrumenten voor de verplichte interne controle ontbraken en mede daardoor was effectief extern toezicht door de CTIVD nog onvoldoende geborgd. De AIVD en de MIVD dienden op korte termijn binnen hun organisaties concrete stappen te zetten om in de praktijk te waarborgen dat aan de eisen uit de Wiv 2017 wordt voldaan.

### Voortgangsrapportage II

In juni 2019 volgde de tweede voortgangsrapportage over de invoering van de Wiv 2017. De CTIVD constateerde dat de AIVD en de MIVD de achterstand bij de invoering van deze nieuwe wet voor een deel hadden ingelopen. De AIVD en de MIVD hadden hard gewerkt aan de invoering van wettelijke waarborgen voor de rechtsbescherming van de burger en lieten blijken doordrongen te zijn van de noodzaak van interne controle op de naleving van de wet. De meeste hoge risico's voor onrechtmatig handelen uit de eerste voortgangsrapportage van de CTIVD waren door de beide diensten teruggebracht naar gemiddelde of beperkte risico's. De CTIVD stelde ook vast dat de diensten er nog niet waren en ook de daaropvolgende tijd nog veel werk te verzetten hadden.

1 Verzoek minister BZK i.v.m. moties en toezeggingen Wiv 2017, d.d. 25 april 2018, *Kamerstukken II* 2017/18, 34588 nr. 1 (bijlage).

## Voortgangsrapportage III

De AIVD en de MIVD hebben naar aanleiding van de eerste voortgangsrapportage ieder een zogenoemde 'Wiv board' ingesteld binnen hun organisaties. Hiermee is beoogd de door de CTIVD geconstateerde risico's integraal en structureel aan te pakken. Deze Wiv-boards zijn ook na de tweede voortgangsrapportage gecontinueerd. De CTIVD heeft de activiteiten van de Wiv boards van de beide diensten op de voet gevolgd en heeft met regelmaat reflectie daarop gegeven. Dit omvatte onder meer een toetsbare tijdsplanning, nieuw opgesteld beleid en werkinstructies, de inrichting van werkprocessen en technische systemen en de verdere uitwerking van een systematiek voor *compliance* en interne controle, waarmee ook effectief extern toezicht door de CTIVD geborgd moet zijn. De concrete stappen die de beide diensten hebben gezet, worden benoemd in deze derde voortgangsrapportage. Deze richt zich op de volgende onderwerpen:

1. het bestaan van het toegezegde instrumentarium voor de **zorgplicht** van de diensten voor een **rechtmatige gegevensverwerking** en de werking van dat instrumentarium;
2. de wijze waarop voortdurende **datareductie** plaatsvindt bij de verwerking van met bijzondere bevoegdheden verzamelde gegevens, waarbij centraal staat de toepassing van de plicht gegevens zo spoedig mogelijk op relevantie te beoordelen en niet relevante gegevens (terstond) te vernietigen (datareductie bij onderzoeksopdrachtgerichte interceptie valt hier buiten);
3. de inzet van de bevoegdheid van **onderzoeksopdrachtgerichte interceptie**, waaronder de toepassing van het criterium 'zo gericht mogelijk', datareductie in de verschillende fasen van verwerking, en de inzet van **geautomatiseerde metadata-analyse** ex. artikel 50; en
4. de **samenwerking met buitenlandse diensten**, waaronder het bestaan en de werking van wegingsnotities.

De CTIVD heeft in het afgelopen half jaar drie toezichtrapporten gepubliceerd die voor een deel overeenkomen met de hierboven staande onderwerpen. Het betreft:

5. de zo gericht mogelijke verzameling van gegevens door de **toepassing van filters** en de zo gericht mogelijke verwerking van gegevens bij de **inzet van de selectiebevoegdheid** in het kader van het stelsel van onderzoeksopdrachtgerichte interceptie; en
6. de verstrekking van **ongeëvalueerde gegevens** aan buitenlandse diensten.

Verder heeft de CTIVD met de inzet van haar ICT unit een start gemaakt met twee technische steekproeven, teneinde de werking van processen en systemen in de praktijk te toetsen:

7. steekproef naar de **werking van het datareductie systeem**; en
8. steekproef naar **geautomatiseerde metadata-analyse** ex. artikel 50 Wiv 2017.

## Toelichting

In het kader van de voortgang heeft de CTIVD marginaal getoetst of de wettelijke en toegezegde beleidsmatige waarborgen voor de rechtsbescherming van de burger een nadere invulling hebben gekregen in het beleid en de werkprocessen van de AIVD en de MIVD en in de inrichting van technische systemen bij de gegevensverwerking. Deze beoordelingen betreffen een inschatting van risico's op onrechtmatig handelen en niet het oordeel dat daarmee daadwerkelijk onrechtmatig is gehandeld. De beoordeling van de rechtmatigheid van de praktijk vindt voornamelijk plaats in de diepteonderzoeken van de CTIVD en krijgt dan zijn weerslag in toezichtsrapporten. Waar relevant wordt in deze derde voortgangsrapportage benoemt wat in de kern de bevindingen van de CTIVD zijn op basis van verrichte diepteonderzoeken.

## Leeswijzer

**Hoofdstuk 2** geeft een algemeen beeld van de voortgang die de AIVD en de MIVD in het afgelopen half jaar hebben bereikt. Ook wordt in dat verband nader ingegaan op de hierboven onder punt 1 t/m 4 genoemde onderwerpen: de zorgplicht, datareductie, onderzoeksopdrachtgerichte interceptie en internationale samenwerking. De voortgang wordt beschreven en de bijbehorende risico's op onrechtmatigheden worden kort weergegeven. De CTIVD heeft er voor gekozen de risico's niet nader toe te lichten in een bijlage. De CTIVD verwijst hiervoor naar de bijlage bij de tweede voortgangsrapportage, beschikbaar op www.ctivd.nl. **Hoofdstuk 3** behandelt de start die is gemaakt door de ICT unit van de CTIVD met een (technische) steekproef naar de werking van het datareductie systeem en een steekproef die is verricht naar geautomatiseerde metadata-analyse. **Hoofdstuk 4** zet uiteen wat de komende tijd van de CTIVD verwacht kan worden. De CTIVD blijft de verdere voortgang op de voet volgen. Zij zal hierover in concluderende zin rapporteren in haar vierde en laatste voortgangsrapportage die wordt vastgesteld in mei 2020.

# 2 Voortgang bij de diensten

## 2.1 Algemeen beeld

In de Wiv 2017 is een werkbare juridische balans gevonden tussen de noodzakelijke bevoegdheden die in het belang van de nationale veiligheid door de AIVD en de MIVD kunnen worden ingezet en de waarborgen voor de rechtsbescherming van de burger die daarbij aan de orde zijn. Een zelfde balans moet ook in de praktijk worden gerealiseerd. Het is de opdracht aan de beide diensten de uitvoering van hun vergaande bevoegdheden en de gegevensverwerking die daarmee gepaard gaat, te voorzien van voldoende rechtens relevante *checks* en *balances*. De CTIVD constateerde in haar eerste voortgangsrapportage van december 2018 dat sprake was van een disbalans, vanwege een achterstand bij de implementatie van wettelijke waarborgen door de beide diensten. In de periode daarna hebben de AIVD en de MIVD de door de CTIVD geconstateerde risico's serieus opgepakt en concrete stappen gezet deze weg te nemen. De CTIVD constateerde in haar tweede voortgangsrapportage van juni 2019 dat de achterstand bij de invoering van de wet voor een deel was ingelopen. De beide diensten hadden hard gewerkt en concrete resultaten bereikt, maar waren er zeker nog niet.

De CTIVD komt nu in deze derde voortgangsrapportage tot dezelfde risicoduiding. Er is veel werk verzet, maar aan de noodzakelijke wettelijke waarborgen voor de rechtsbescherming van de burger wordt nog onvoldoende invulling gegeven. Er is nog steeds sprake van aanzienlijke risico's op onrechtmatig handelen. De belangrijkste stappen die door de diensten (voort)gezet moeten worden, zijn het omzetten van wetgeving en beleid in concrete instructies voor medewerkers, interne processen, technische systemen en adequate interne controlemechanismen. Zodat het ook in de praktijk werkt zoals het hoort te werken en intern en extern controleerbaar is. Dit zijn randvoorwaarden waaraan de AIVD en de MIVD moeten voldoen, voor zowel de rechtmatigheid van hun activiteiten als voor de toetsbaarheid daarvan.

De techniekonafhankelijke formulering van de Wiv 2017 maakt dat de AIVD en de MIVD het nodige moeten doen om de wet in de praktijk tot uitvoering te brengen. Daarbij is het aanpassen van de werkwijze en technische werkomgeving van de diensten noodzakelijk. Gelet op de complexiteit van de datahuishouding en ICT infrastructuur bij beide diensten, is dit niet eenvoudig of snel te realiseren. Bovendien lopen de AIVD en de MIVD in de praktijk steeds meer tegen de situatie aan dat de huidige inrichting van de werkprocessen en systemen onvoldoende is toegesneden op de vereisten die de wet stelt. Het aanpassen hiervan blijkt dan veelomvattender dan aanvankelijk gedacht. Dit vraagt ook om een cultuurverandering, waarvan de eerste effecten binnen de organisaties zichtbaar zijn.

De AIVD en de MIVD hebben de implementatie van de wet het afgelopen half jaar dan ook niet met een zelfde stijgende lijn kunnen voortzetten als bij de tweede voortgangsrapportage het geval was. Wel zijn fundamentele veranderingen in gang gezet, wordt er hard gewerkt en zijn de inzet en bereidheid volop aanwezig. Ook is de onderlinge samenwerking tussen de diensten bij de implementatie van de wet versterkt, waardoor meer uniformiteit in de werkprocessen ontstaat. De benodigde resultaten zijn echter nog niet voldoende behaald. De risico's die zijn benoemd in de tweede voortgangsrapportage zijn in deze derde voortgangsrapportage dan ook ongewijzigd gebleven.

Inmiddels is ruim anderhalf jaar verstreken sinds de inwerkingtreding van de Wiv 2017 in mei 2018. De belangrijkste nieuwe bevoegdheid tot onderzoeksopdrachtgerichte interceptie op de kabel is nog niet ingezet. De huidige stand van zaken roept echter de vraag op of de AIVD en de MIVD er klaar voor zijn de kabel in bulk te intercepteren. De CTIVD stelt hier randvoorwaarden bij (zie ook paragraaf 2.4).

De implementatie van de Wiv 2017 vergt veel van de AIVD en de MIVD. Zowel in het politiek als in het maatschappelijk debat klinkt in dit verband soms de gedachte door dat de administratieve last, die

deze implementatie met zich meebrengt, wel eens ten koste zou kunnen gaan van de operationele slagkracht van de beide diensten. Hoewel de CTIVD vooralsnog geen concrete aanwijzingen heeft dat dit aan de orde is, ziet zij wel dat operationele capaciteit wordt aangewend voor de implementatie van de Wiv 2017. Zij acht een onafhankelijke beoordeling van de impact van de nieuwe wet op de operationele taakuitvoering door de AIVD en de MIVD dan ook raadzaam. Indien inderdaad blijkt van een permanente administratieve lastenverzwaring, dienen hier passende maatregelen tegenover te staan. Vanzelfsprekend kan hierbij geen sprake zijn van een vermindering van de waarborgen voor de rechtsbescherming van de burger. Omdat een dergelijk onderzoek buiten de reikwijdte van haar toezicht valt, heeft de CTIVD het belang van een dergelijk doelmatigheidsonderzoek onder de aandacht van de Algemene Rekenkamer gebracht.

## 2.2 Voortgang m.b.t. de zorgplicht

### Achtergrond

De wettelijke zorgplicht van de AIVD en de MIVD voor een rechtmatige gegevensverwerking houdt in dat de beide diensten zélf voortdurend controle uitoefenen op de wijze waarop zij gegevens verwerken. Zij moeten er zélf voor zorgen dat zij voldoen aan de wet (*compliance*) en dat ook blijven doen. Dit vereist onder meer het gebruik van instrumenten die hen (centraal) zicht geven op de werking van processen en systemen van gegevensverwerking en hen daardoor in staat stellen risico's te signaleren en tijdig maatregelen te nemen. Een goede inrichting van de zorgplicht draagt niet alleen bij aan *compliance* maar dient ook de professionaliteit en de operationele integriteit van de beide diensten. Adequate interne controle door de diensten is bovendien ook essentieel voor het effectief kunnen verrichten van extern toezicht door de CTIVD.

De CTIVD heeft in haar eerste voortgangsrapportage geconstateerd dat er geen instrumentarium voor de zorgplicht aanwezig was bij de AIVD en de MIVD. In de tweede voortgangsrapportage stelde de CTIVD vast dat de beide diensten een instrumentarium op hoofdlijnen hadden vastgesteld. De AIVD had hier bovendien concrete invulling en uitvoering aan gegeven, onder meer door het verrichten van enkele risicoanalyses van werkprocessen voor de inzet en toepassing van (bijzondere) bevoegdheden en een audit naar de systematiek van datareductie. Bij de MIVD waren nog weinig stappen gezet om het instrumentarium nader in te richten en toe te passen.

### Voortgang AIVD

De AIVD heeft verdere voortgang geboekt met de inbedding van de zorgplicht in de interne organisatie. Het besluit is genomen een stelsel voor de zorgplicht en de naleving van wettelijke vereisten (*compliance*) structureel onderdeel te laten uitmaken van de administratieve organisatie en niet slechts tijdelijk ten behoeve van de implementatie van de nieuwe wet. De concrete uitwerking van dit stelsel is inmiddels afgerond en moet nu verder worden ingericht binnen de AIVD; onder meer door het aanstellen van personen, het beleggen van verantwoordelijkheden en het inrichten van interne processen voor risico- en *compliance* management. De AIVD is verder gegaan met het verrichten van risicoanalyses van werkprocessen voor de inzet en toepassing van (bijzondere) bevoegdheden. Naar aanleiding van deze risicoanalyses zijn en worden technische, personele en/of organisatorische maatregelen in gang gezet. Ook is gestart met een tweede audit op datareductie. In de tijdsplanning voor de komende tijd is opgenomen dat de AIVD het verrichten van risicoanalyses zal continueren. Verder wordt beoogd een systematiek voor *compliance* met behulp van dashboards uit te werken.

**Risico indicatie**
Het risico op onrechtmatig handelen wordt gehandhaafd op **beperkt**.

### Voortgang MIVD

Ook bij de MIVD is het besluit genomen een stelsel voor de zorgplicht en de naleving van wettelijke vereisten (*compliance*) structureel onderdeel te maken van de administratieve organisatie. Dit stelsel moet echter op onderdelen nog verder worden uitgewerkt. Er is besloten de Wiv-board een permanent onderdeel van het bestuur van de MIVD te laten uitmaken. Ook heeft de MIVD geïnvesteerd in het verder in kaart brengen van de eigen werkprocessen, teneinde deze te verbeteren. De MIVD beoogt in 2020 een kwaliteit management systematiek te implementeren, wat ook als hulpmiddel kan fungeren bij het inrichten van *compliance* binnen de organisatie. Verder is een interne enquête opgezet, aan de hand waarvan de teams en bureaus van de MIVD op specifieke onderdelen moeten aangeven of zij bepaalde wettelijke en beleidsmatige verplichtingen zijn nagekomen. Op basis hiervan kan door afdelingshoofden nadere sturing en controle plaatsvinden, binnen de reguliere verantwoordingslijn. De systematiek van risicoanalyses is overgenomen van de AIVD. Een aantal risicoanalyses op werkprocessen voor de inzet en toepassing van (bijzondere) bevoegdheden is inmiddels in gang gezet. De resultaten hiervan worden tussen de beide diensten uitgewisseld en besproken. Ook zijn er stappen gezet om een *compliance* structuur in te richten binnen de MIVD. Dit moet op korte termijn nader vorm krijgen binnen de MIVD.

**Risico indicatie**
Het risico op onrechtmatig handelen wordt gehandhaafd op **gemiddeld**.

## 2.3 Voortgang m.b.t. datareductie

### Achtergrond

De AIVD en de MIVD moeten op basis van artikel 27 Wiv 2017 de gegevens die zij verzamelen door middel van bijzondere bevoegdheden zo spoedig mogelijk op relevantie beoordelen. Niet relevante gegevens moeten terstond en onomkeerbaar worden vernietigd. Gegevens die niet zijn beoordeeld op relevantie moeten binnen een jaar na verwerving zijn vernietigd. Hierbij is een verlenging van de bewaartermijn mogelijk van een half jaar. Gegevens verzameld door onderzoeksopdrachtgerichte interceptie vallen buiten deze regeling. Daarvoor geldt een bewaartermijn van maximaal drie jaar.

In de eerste voortgangsrapportage constateerde de CTIVD onder meer dat beleid en werkinstructies op essentiële onderdelen ontbraken, de vernietiging van gegevens nog niet (volledig) geborgd was en interne controle en daarmee effectief toezicht niet aan de orde waren. Bij de MIVD was een beperkt ondersteunende ICT infrastructuur hier mede debet aan. De tweede voortgangsrapportage gaf een positiever beeld. Beleid en werkinstructies waren grotendeels op orde. Er was voortgang bereikt met het zo spoedig mogelijk op relevantie beoordelen van gegevens, waaronder gegevens verzameld op basis van de Wiv 2002. Daarnaast had de AIVD concrete stappen gezet met het implementeren van de datareductie systematiek in de technische systemen.

### Voortgang AIVD

Het beleid en de werkinstructies op het gebied van datareductie zijn grotendeels op orde. Het beleid dient nog een verdere (technische) vertaalslag te krijgen in de applicaties die door medewerkers van de AVD gebruikt worden voor de verwerking van gegevens. De relevantie beoordeling van Wiv 2002 data is grotendeels afgerond (zie verder onder bulkdatasets) en heeft geleid tot vernietiging van niet relevante gegevens. De AIVD is bezig met het inrichten van interne controlemechanismen. Er is inmiddels een audit verricht t.a.v. datareductie. Een tweede audit is onlangs gestart. Op de concrete werking van het datareductie systeem wordt nader ingegaan in paragraaf 3.2, waar de voorlopige bevindingen worden weergegeven van de steekproef die de CTIVD heeft verricht.

De CTIVD ziet in de uitvoering van de wettelijke plicht tot datareductie bij de AIVD (en ook bij de MIVD) knelpunten ontstaan in het binnen de wettelijke termijn van maximaal anderhalf jaar op relevantie beoordelen van bulkdatasets en in de wijze waarop de relevantiebeoordeling in de praktijk impliciet kan plaatsvinden. Zij bespreekt dit hieronder afzonderlijk.

**Risico indicatie**
Het eerder geconstateerde **gemiddelde** risico m.b.t. de wijze waarop relevantiebeoordeling plaatsvindt, wordt gehandhaafd. Voor het overige blijven de risico's op onrechtmatig handelen **beperkt**. Een uitzondering hierop vormt het zo spoedig mogelijk op relevantie beoordelen van bepaalde bulkdatasets. Hier is geen sprake meer van een risico maar van een onrechtmatigheid.

### Voortgang MIVD

Het beleid en de werkinstructies op het gebied van datareductie zijn grotendeels op orde. Problematisch bij de MIVD blijft de technische implementatie van wet en beleid, die moet ondersteunen dat gegevens zo spoedig mogelijk op relevantie beoordeeld worden en niet relevante gegevens terstond vernietigd worden. De MIVD is in april 2019 begonnen met een ICT-pilot gericht op het ontwikkelen van een moderne data architectuur. De herinrichting van het ICT-landschap is een meerjarig traject waarvan de einddatum nog niet is vastgesteld. De eerste projecten in dit kader zijn aangevangen en kunnen op onderdelen ook op kortere termijn effect hebben.

Er is gedeeltelijk voorzien in de geautomatiseerde vernietiging van gegevens bij het verlopen van de bewaartermijn van maximaal anderhalf jaar (inclusief verlenging). Op dit terrein is beperkte voortgang bereikt het afgelopen half jaar. Verder is hard gewerkt aan een mogelijkheid MIVD gegevens op AIVD systemen op relevantie te kunnen beoordelen. Hier lijkt een technische oplossing voor te zijn gevonden. Interne controle op het datareductie proces is nog niet gerealiseerd. Zo wordt niet gecontroleerd of de vernietiging van Wiv 2002 gegevens voor 1 november 2019 daadwerkelijk is afgerond. Ditzelfde geldt voor gegevens verworven op basis van de Wiv 2017 waarvan de bewaartermijn inmiddels is verstreken.

**Risico indicatie**
De CTIVD handhaaft de eerder geconstateerde risico's op **beperkt** (wat wordt verstaan onder relevantie en op welke termijn wordt beoordeeld) en **hoog** (wijze waarop relevantieboordeling en onomkeerbare vernietiging plaatsvindt). Een uitzondering hierop vormt het zo spoedig mogelijk op relevantie beoordelen van bepaalde bulkdatasets. Hier is geen sprake meer van een risico maar van een onrechtmatigheid.

### Voortgang AIVD en MIVD

*Relevantiebeoordeling bulkdatasets*
Bulkdatasets zijn grote gegevensverzamelingen waarvan het merendeel van de gegevens betrekking heeft op organisaties en/of personen die geen onderwerp van onderzoek van de diensten zijn en dat ook nooit zullen worden. Dergelijke bulkdatasets kunnen bijvoorbeeld met de hackbevoegdheid of met de inzet van informanten worden binnengehaald. Voor de verzameling en verdere verwerking van deze bulkdatasets is geen specifieke wettelijke regeling opgenomen.

De belangrijkste waarborg voor de rechtsbescherming van de burger is het vereiste dat de gegevens binnen een jaar (eventueel met een verlenging van een half jaar) op relevantie beoordeeld moeten worden. Dit vereiste is echter in de praktijk niet goed uitvoerbaar. Het gaat om te veel gegevens. Na een jaar moet datgene wat niet als relevant is beoordeeld vernietigd worden. Dergelijke bulkdatasets zijn, vanwege de specifieke aard daarvan, echter aanzienlijk langer van waarde voor de onderzoeken van de diensten dan een jaar.

Het betreft zowel datasets die op basis van de Wiv 2017 zijn verworven als datasets die nog onder de oude wet, de Wiv 2002, zijn binnengehaald. De datasets zijn verworven door de AIVD, maar worden ook door de MIVD gebruikt. Voor deze bulkdatasets is in april 2019 door de AIVD de beslissing genomen de bewaartermijn met een half jaar te verlengen. Dit besluit is door de MIVD onderschreven. De betrokken minister is hier destijds over geïnformeerd. Deze gegevens dienden nu voor 1 november 2019 relevant beoordeeld dan wel vernietigd te zijn. De AIVD heeft het afgelopen half jaar een grote uitdaging gehad met het op relevantie beoordelen hiervan. Het betreft een aanzienlijke hoeveelheid gegevens die in ieder geval gedeeltelijk nog steeds noodzakelijk is voor de taakuitvoering van de diensten. Integrale vernietiging van de bulkdatasets zou voor de beide diensten tot operationele risico's kunnen leiden.

De AIVD is er niet in geslaagd de gegevens in de bulkdatasets inhoudelijk op relevantie te beoordelen. Wel heeft de dienst een analyse verricht ten aanzien van onder meer de aard en kwaliteit van de gegevens en het gebruik van de gegevens in het inlichtingenproces. Op basis van deze analyse is een algemeen beeld verkregen van de waarde van de bulkdatasets in hun geheel. Aan de hand hiervan is er voor gekozen een deel van de bulkdatasets geheel te vernietigen, van een deel van de bulkdatasets een onderdeel te vernietigen en het overige te bewaren en een deel van de bulkdatasets in hun geheel te bewaren. De bewaarde gegevens zijn integraal als relevant aangemerkt. Inherent aan de bulkdatasets is echter dat zij gegevens bevatten waarvan het overgrote deel betrekking heeft op organisaties en/of personen die geen onderwerp van onderzoek van de diensten zijn en dat ook nooit zullen worden. Dit zijn gegevens die niet relevant zijn voor de taakuitvoering, maar wel als zodanig zijn aangemerkt.

Om te voorkomen dat deze gegevens zonder meer beschikbaar komen voor de operationele teams en gebruikt kunnen worden in het operationeel proces, zijn door de AIVD en de MIVD aanvullende waarborgen ingesteld. De bulkdatasets zijn niet voor iedereen toegankelijk, maar kunnen door medewerkers van de operationele teams worden bevraagd door middel van gerichte zoekslagen. Wanneer een zoekslag resultaten oplevert, moet intern toestemming worden verkregen voor het kennisnemen van de desbetreffende gegevens.

Waar het gaat om de als relevant aangemerkte bulkdatasets kan niet meer worden gesproken van een risico op onrechtmatig handelen. De CTIVD beoordeelt de beslissing van de AIVD de desbetreffende (delen van) bulkdatasets als relevant aan te merken en dus te bewaren als onrechtmatig. De Wiv 2017 biedt hier geen ruimte voor. De CTIVD onderschrijft de operationele belangen van de AIVD en de MIVD een deel van de bulkdatasets die zijn verworven te bewaren. Ook heeft zij begrip voor de beperkte haalbaarheid binnen een termijn van een jaar (of bij verlenging anderhalf jaar) de bulkdatasets inhoudelijk op relevantie te beoordelen. De wet vereist dit echter wel. Gegevens die niet binnen die termijn zijn beoordeeld, moeten worden vernietigd.

Hoewel het positief is dat de beide diensten zichzelf aanvullende waarborgen hebben opgelegd bij het gebruik van bulkdatasets, voldoet dit niet zonder meer. Trekt men de vergelijking met de bevoegdheid van onderzoeksopdrachtgerichte interceptie waarmee eveneens gegevens in bulk kunnen worden verzameld, dan zijn in dat verband striktere waarborgen voor de rechtsbescherming van de burger aan de orde. Bij onderzoeksopdrachtgerichte interceptie is voorzien in externe toestemming en onafhankelijke toetsing voorafgaand aan de kennisname en analyse van de gegevens en dient vernietiging van de gegevens die niet als relevant zijn aangemerkt binnen drie jaar plaats te vinden. In het geval van de bulkdatasets is niet voorzien in externe toestemming en onafhankelijke toetsing voorafgaand aan het gebruik van de gegevens. Belangrijker nog, als gevolg van het relevant aanmerken van (delen van) de bulkdatasets is een definitieve vernietigingstermijn voor de gegevens komen te vervallen, terwijl de gegevens niet inhoudelijk beoordeeld zijn. Evenmin is sprake van andere waarborgen die afdoende rechtsbescherming bieden.

*Impliciete relevantiebeoordeling*
In de toelichting bij de wet en de parlementaire behandeling ervan is niet stilgestaan bij de wijze waarop de verplichte relevantiebeoordeling moet plaatsvinden en de eisen die aan die beoordeling mogen worden gesteld. De in de toelichting bij de wet genoemde voorbeelden wijzen op een expliciete relevantiebeoordeling, dat wil zeggen een beoordeling van de inhoud van de gegevens. Zo dient een telefoontap uitgeluisterd te worden om te bepalen welke gegevens wel of niet relevant zijn. Bij gegevens verworven door onderzoeksopdrachtgerichte interceptie is sprake van een getrapte relevantiebeoordeling. In elke fase van het interceptiestelsel krijgt de relevantiebeoordeling een andere invulling en dienen niet relevante gegevens te worden vernietigd. Van relevante gegevens kan in beginsel pas sprake zijn wanneer de feitelijke inhoud van de communicatie is beoordeeld.

De AIVD en de MIVD passen in de praktijk in bepaalde gevallen een impliciete relevantiebeoordeling toe, ook wel relevantiebeoordeling vooraf. Bij de aanvraag van een bijzondere bevoegdheid kan vooraf worden aangegeven dat de opbrengst van de inzet behorend bij een bepaald (technisch) kenmerk (bijv. een telefoonnummer) in zijn geheel als relevant kan worden aangemerkt. De gegevens die worden verzameld t.a.v. dat kenmerk, worden vervolgens automatisch als relevant gelabeld. De CTIVD ziet geen wettelijke ruimte voor het categorisch op voorhand als relevant aanmerken van gegevens die worden verworven met de inzet van bijzondere bevoegdheden. Het categorisch op voorhand als relevant aanmerken van nog te verwerven gegevens brengt immers een aanzienlijk risico met zich mee dat niet relevante gegevens bewaard zullen worden.

De CTIVD heeft hierover nader overleg gevoerd met de AIVD en de MIVD, ten aanzien van díe uitzonderingsgevallen waarin impliciete relevantiebeoordeling wél aan de orde kan zijn en de waarborgen die dan van toepassing moeten zijn. Een belangrijke voorwaarde is het expliciet motiveren waarom de verwachting bestaat dat de inzet op een (technisch) kenmerk uitsluitend relevante gegevens zal opleveren. Dit dient plaats te vinden op basis van de kennis die de dienst heeft van het desbetreffende (technisch) kenmerk en het daaraan gekoppelde target van de dienst. Wanneer bijvoorbeeld een baken wordt geplaatst onder een voertuig en dit gegevens oplevert over het verplaatsingsgedrag, kunnen de gegevens slechts op voorhand als relevant worden aangemerkt indien gemotiveerd kan worden dat uitsluitend het target waarnaar de dienst onderzoek verricht in het voertuig heeft gereden. De impliciete relevantiebeoordeling is in beginsel uitgesloten bij het gebruik van nieuwe (technische) kenmerken (en de diensten dus nog onvoldoende kennis hebben van het gebruik ervan) of kenmerken die beperkt gericht zijn op een persoon of organisatie. Overige voorwaarden die de CTIVD stelt, zien op het vervroegd beoordelen of de verworven gegevens nog van betekenis voor de taakuitvoering zijn en op het voorzien in interne controle. De beide diensten onderschrijven dit en zijn bezig met het nader uitwerken en (technisch) implementeren van het bovenstaande.

## 2.4 Voortgang m.b.t. onderzoeksopdrachtgerichte interceptie

**Achtergrond**
De Wiv 2017 geeft de mogelijkheid zowel via de ether als op de kabel (persoons)gegevens te verzamelen in grote hoeveelheden (bulk) en deze verder te verwerken. Belangrijke waarborgen voor de rechtsbescherming van de burger zijn onder meer dat de bevoegdheden, ook in het kader van onderzoeksopdrachtgerichte interceptie, zo gericht mogelijk worden toegepast en de verworven gegevens binnen de bewaartermijn van maximaal drie jaar worden beperkt tot die gegevens die relevant zijn voor het uitvoeren van de onderzoeksopdrachten van de beide diensten. Deze datareductie vindt in het stelsel van onderzoeksopdrachtgerichte interceptie getrapt plaats en onderscheidt zich daarmee van de in paragraaf 2.3 besproken datareductie op basis van artikel 27 Wiv 2017.

De CTIVD heeft in haar eerste voortgangsrapportage onder meer geconstateerd dat geen herkenbare invulling werd gegeven aan het criterium ‘zo gericht mogelijk’, geen specifiek beleid was vastgesteld

voor databeperking en het onduidelijk was hoe dit binnen het interceptiestelsel plaatsvond, interne controle op deze processen ontbrak en daarmee effectief toezicht niet mogelijk was. In de tweede voortgangsrapportage stelde de CTIVD vast dat de diensten hun beleid en werkinstructies hadden verbeterd hoewel op onderdelen nog werkinstructies ontbraken, in het bijzonder voor de toepassing van filters. Een zorgpunt was bovendien het vooraf als relevant aanmerken van gegevens die met 'gerichte' selectiecriteria zijn geselecteerd, zonder dat een inhoudelijke beoordeling van de gegevens daaraan ten grondslag ligt.

De CTIVD publiceerde begin september 2019 haar toezichtsrapport nr. 63 over de toepassing van filters bij onderzoeksopdrachtgerichte interceptie. Medio oktober volgde rapport nr. 64 over de toepassing van de selectiebevoegdheid. Beide toezichtsrapporten geven aan dat de hoge risico's die de CTIVD in periode van de eerste voortgangsrapportage constateerde, zich voor een deel hebben gemanifesteerd door middel van onrechtmatigheden. Het gerichtheidsvereiste dient nadrukkelijk een betere toepassing te krijgen in de praktijk, zowel bij de toepassing van filters als bij selectie. Bij de AIVD leidden interne technische problemen met een deel van de interceptie- en selectieketen tot het gedeeltelijk stopzetten van de toepassing van selectie en daarmee voor de CTIVD tot een beperkt beeld van de praktijk. Bij de MIVD constateerde de CTIVD onder meer dat niet-relevante gegevens ten onrechte niet vernietigd waren.

### Voortgang AIVD en MIVD

De AIVD en de MIVD hebben een gezamenlijk verbeterprogramma opgezet voor onderzoeksopdracht gerichte interceptie. Dit verbeterprogramma richt zich op de risico's die door de CTIVD zijn geconstateerd in haar voortgangsrapportages, de aanbevelingen van de CTIVD in de rapporten 63 en 64, de selectieproblematiek die de AIVD zelf heeft ervaren en de uitkomst van een risicoanalyse die inmiddels is verricht door de beide diensten.

Het verbeterprogramma heeft onder meer tot doel het beleid, de werkinstructies en de procesbeschrijvingen te actualiseren en/of aan te vullen. Duidelijk moet zijn wie, wat, wanneer doet in het stelsel van onderzoeksopdrachtgerichte interceptie. Ook wordt in dit verband aandacht besteed aan opleidingen en informatievoorziening aan medewerkers. Daarnaast is het programma nadrukkelijk gericht op het verder op orde brengen van de technische verwerkingssystemen voor onderzoeksopdrachtgerichte interceptie. Technische systemen die onderdeel uitmaken van de interceptieketen moeten beschikbaar zijn, naar behoren werken en invulling geven aan de wettelijke vereisten. Het verbeterprogramma is qua opzet en uitvoering veelbelovend en zou eind 2019 afgerond moeten zijn. De CTIVD zal hier dan ook uitgebreider op ingaan in haar vierde en laatste voortgangsrapportage die wordt vastgesteld in mei 2020. De CTIVD hoopt tegen die tijd ook een eerste beeld te kunnen schetsen van de feitelijke toepassing van de bevoegdheid tot onderzoeksopdrachtgerichte interceptie van de kabel.

*Bulkinterceptie van de kabel*

Los van enkele verkennende activiteiten, waarvoor toestemming is verkregen, heeft er vooralsnog geen onderzoeksopdrachtgerichte interceptie van de kabel plaatsgevonden. Een wezenlijke vraag is of de AIVD en de MIVD klaar zijn voor de inzet van onderzoeksopdrachtgerichte interceptie van de kabel. De wettelijke waarborgen voor de rechtsbescherming van de burger dienen niet alleen in beleid, maar ook in werkprocessen en technische systemen geïmplementeerd te zijn. Bovendien is het zaak dat in de uitvoeringspraktijk de 'juiste knoppen op de juiste stand' worden gezet, zodat de kabel daadwerkelijk zo gericht mogelijk wordt geïntercepteerd en vervolgens het kaf van het koren wordt gescheiden. Ook moet adequate interne controle aan de orde zijn en daarmee mogelijkheden voor effectief toezicht door de CTIVD. De vraag of hieraan wordt voldaan voordat onderzoeksopdrachtgerichte interceptie van de kabel plaatsvindt, moet in eerste instantie door de beide diensten zelf worden beantwoord en zal door de CTIVD worden getoetst.

Randvoorwaardelijk hiervoor is dat het eerder genoemde verbeterprogramma tot voldoende resultaat leidt. De risico's met betrekking tot de zo gericht mogelijke inzet en toepassing van bevoegdheden en de verantwoorde datareductie in het stelsel van onderzoeksopdrachtgerichte interceptie, dienen aanzienlijk verminderd te zijn. Dit betekent onder meer ook dat de inrichting van technische systemen en de wijze waarop deze worden toegepast moeten voorzien in de wettelijke vereiste rechtsbescherming van de burger bij onderzoeksopdrachtgerichte interceptie. Bovendien moet het stelsel voldoende toetsbaar zijn. Dit vereist onder meer het gebruik van instrumenten die de diensten (centraal) zicht geven op de werking van processen en systemen in het kader van onderzoeksopdrachtgerichte interceptie en hen daardoor in staat stellen risico's te signaleren en tijdig maatregelen te nemen. De CTIVD heeft de resultaten van het verbeterprogramma tot dusver nog niet kunnen beoordelen. Zij zal hier de komende tijd aandacht aan besteden. De CTIVD wijst in dit verband ook op de paragrafen 2.5 en 3.3 waarin de praktijk en controleerbaarheid van geautomatiseerde data-analyse wordt besproken en op paragraaf 2.6, waarin wordt stilgestaan bij de verstrekking van ongeëvalueerde gegevens. De AIVD en de MIVD hebben op dit vlak nadrukkelijk nog een grote uitdaging.

**Risico indicatie**
De eerder geconstateerde risico's worden voor de beide diensten gehandhaafd op **gemiddeld** (zo gericht mogelijk en datareductie) en **beperkt** (selectie en functie- en taakscheiding).

## 2.5 Voortgang m.b.t. geautomatiseerde data-analyse

### Achtergrond

In het politiek en maatschappelijk debat rond de Wiv 2017 is er veel aandacht geweest voor metadata-analyse en de mate waarin dit een inmenging vormt in de persoonlijke levenssfeer van de burger. In artikel 50 Wiv 2017 is vastgelegd dat de AIVD en de MIVD toestemming moeten hebben van de betrokken minister als zij personen of organisaties willen identificeren via de geautomatiseerde analyse van metadata die zijn verkregen door onderzoeksopdrachtgerichte interceptie (geautomatiseerde data-analyse). Deze toestemming wordt vervolgens op rechtmatigheid getoetst door de TIB. Pas dan mag de bevoegdheid worden toegepast. De toepassing van deze vorm van geautomatiseerde data-analyse maakt onderdeel uit van het stelsel van onderzoeksopdrachtgerichte interceptie.

Voor alle overige vormen van geautomatiseerde data-analyse geldt artikel 60 Wiv 2017. Dit omvat een breed palet aan gegevensverwerkingen die geautomatiseerd plaatsvinden en die behoren tot de dagelijkse activiteiten van de AIVD en de MIVD. Het gaat daarbij om simpele zoekslagen, maar ook om ingewikkelde technieken als *profiling*. Toestemming van de betrokken minister en een toetsing daarvan door de TIB zijn hierbij niet wettelijk vereist.

De CTIVD heeft in haar eerste voortgangsrapportage geconstateerd dat het proces van geautomatiseerde (meta)data-analyse ex. artikel 50 met onvoldoende (procedurele) waarborgen was omkleed. Zij beoordeelde het risico op onrechtmatig handelen voor de AIVD en de MIVD als hoog. In de tweede voortgangsrapportage werd het risico bijgesteld naar gemiddeld. De diensten waren opgeschoven in hun uitleg van de wettelijke regeling en hadden dit in beleid vervat. Ook werden plannen voor interne controle uitgewerkt. Specifiek beleid en werkinstructies ontbraken echter nog. Ditzelfde gold voor geautomatiseerde data-analyse ex. artikel 60. Ook daar constateerde de CTIVD naar aanleiding van een nieuwe nulmeting hoge risico's op onrechtmatig handelen.

### Voortgang AIVD en MIVD

Ook in het afgelopen half jaar is veelvuldig met de beide diensten en met de betrokken departementen gesproken over de toepassing van artikel 50 Wiv 2017. De beide diensten worstelen hiermee. Dit ziet vooral op de mate van abstractie dan wel detail van de verzoeken om toestemming die aan de betrokken

minister(s) en vervolgens de TIB worden voorgelegd. Hoe breder een verzoek is geformuleerd, hoe meer ruimte het de diensten biedt verschillende metadata-analyses te kunnen uitvoeren zonder opnieuw verzoeken in te moeten dienen. De wet biedt daarvoor ruimte, ook gezien de mogelijkheid dat voor een periode van een jaar toestemming kan worden verkregen. Niet voor elke afzonderlijke metadata-analyse is een separaat verzoek om toestemming nodig. Daar staat tegenover dat een verzoek om toestemming wel dusdanig specifiek moet zijn, dat de betrokken minister(s) en de TIB een gedegen afweging kunnen maken over de rechtmatigheid daarvan. Zo moet helder zijn in het kader van welke onderzoeksopdracht, met welk oogmerk en met welk doel metadata-analyse plaatsvindt, welke vormen van analyse daarbij aan de orde zijn en welke gegevensbestanden in de analyse worden betrokken.

Het is zaak dat de juiste mate van abstractie dan wel detail wordt bereikt, waarmee zowel een gedegen rechtmatigheidstoets kan plaatsvinden als voldoende operationele ruimte wordt geboden. De praktijk moet dit uitwijzen. In de praktijk heeft de AIVD nog geen voldoende afgebakend verzoek om toestemming ingediend, aangezien de tot dusver ingediende verzoeken onrechtmatig zijn beoordeeld door de TIB. De MIVD heeft in het kader van de ondersteuning van militaire operaties toestemming verkregen deze vorm van geautomatiseerde data-analyse toe te passen.

De diensten hebben aangegeven dat bovenstaande worsteling met de toepassing van de wet ook een reden is waarom specifiek beleid en werkinstructies voor geautomatiseerde data-analyse ontbraken. Dit geldt zowel voor de metadata-analyse op basis van artikel 50 als voor de bredere bevoegdheid van geautomatiseerde data-analyse op basis van artikel 60. Het beleid is inmiddels gereed en vastgesteld door de beide dienstleidingen medio c.q. eind oktober 2019. Door de MIVD is een werkinstructie opgesteld t.b.v. de toepassing van geautomatiseerde data-analyse voor de ondersteuning van een militaire operaties. De CTIVD zal in de vierde en laatste voortgangsrapportage nader hier op in gaan.

In paragraaf 3.3 worden de bevindingen van de tweede steekproef van de CTIVD naar geautomatiseerde data-analyse uiteengezet. Uit de eerste steekproef kwam onder meer naar voren dat geen sprake was van interne controle binnen de diensten en de CTIVD geen effectief toezicht kon uitoefenen.

**Risico indicatie**
Het risico voor de rechtmatige toepassing van geautomatiseerde data-analyse op basis van artikel 50 blijft **gemiddeld**. De eerder geconstateerde risico's voor geautomatiseerde data-analyse op basis van artikel 60 worden voor beide diensten gehandhaafd op **hoog**. Voor de AIVD geldt hier dat sprake is van een **gemiddeld** risico ten aanzien van de controle op de werking van analysetechnieken.

## 2.6 Voortgang m.b.t. internationale samenwerking

### Achtergrond

De CTIVD heeft aspecten van de internationale samenwerking van de AIVD en de MIVD met buitenlandse diensten onderzocht in een tweetal diepteonderzoeken. In februari 2019 is toezichtsrapport nr. 60 gepubliceerd over de wegingsnotities van de AIVD en de MIVD voor de internationale samenwerking met de Counter Terrorism Group- en sigint-partners. De kern hiervan was dat de AIVD en de MIVD in het algemeen tekortschoten in het toetsen aan de wettelijke criteria voor internationale samenwerking. De wegingsnotities voldeden daardoor op onderdelen niet aan de wet.

In oktober 2019 volgde toezichtsrapport nr. 65 over de verstrekking van ongeëvalueerde gegevens aan buitenlandse diensten. In dit deels kaderstellende rapport legde de CTIVD uit wat moet worden verstaan onder geëvalueerde en ongeëvalueerde gegevens. Zij constateerde onder meer dat het beleid en de werkinstructies van de beide diensten op onderdelen verbetering behoefden en dat in de

praktijk zich enige onrechtmatigheden hadden voorgedaan. Het zo snel mogelijk verbeteren van beleid en praktijk is essentieel met het oog op de voorgenomen inzet van de onderzoeksopdrachtgerichte interceptie van de kabel, waarmee meer gegevens kunnen worden verzameld door de beide diensten. De verwachting bestaat dat dan ook steeds meer ongeëvalueerde gegevens zullen worden verstrekt.

Mede naar aanleiding van deze onderzoeken van de CTIVD hebben de AIVD en de MIVD besloten internationale samenwerking aan te merken als nieuwe pijler waarop de Wiv-boards bij de beide diensten integrale sturing geven. Om deze reden bespreekt de CTIVD de voortgang hiervan in deze derde voortgangsrapportage.

### Voortgang AIVD en MIVD

De aanbevelingen uit rapport nr. 60 zijn door de betrokken ministers overgenomen. Zij gaven daarbij aan dat de herziening van de onderzochte wegingsnotities die onrechtmatigheden bevatten uiterlijk 1 juli 2019 zal zijn afgerond. Dit is inmiddels gebeurd. De CTIVD heeft de herziene wegingsnotities nog niet op rechtmatigheid beoordeeld. Dit zal het komende half jaar plaatsvinden. De herziening en actualisering van alle wegingsnotities met betrekking tot overige buitenlandse diensten, mede aan de hand van de aanbevelingen van de CTIVD in rapport nr. 60, wordt door de AIVD afgerond voor 1 juli 2021. Voor de MIVD is vooralsnog niet duidelijk wanneer dit zal zijn afgerond.

De AIVD en de MIVD hebben gezamenlijk gewerkt aan de aanpassing van het beleid, werkinstructies en formats voor de wegingsnotities en hierin uniformiteit aangebracht. Deze aanpassingen worden op korte termijn afgerond.

Voor de verstrekking van ongeëvalueerde gegevens is mede op basis van de aanbevelingen van de CTIVD een verbeterplan opgesteld. De uitvoering hiervan is inmiddels gestart.

De CTIVD zal over beide onderwerpen rapporteren in de vierde voortgangsrapportage.

# 3 Informatiehuishouding en IT-omgeving diensten

## 3.1 Inleiding

De ICT Unit van de CTIVD heeft steekproeven verricht naar de werking van het datareductie systeem ex. artikel 27 Wiv 2017 en de toepassing van geautomatiseerde data-analyse ofwel metadata-analyse ex. artikel 50 Wiv 2017. Dit technisch onderzoek is verricht door specialisten van de CTIVD die in de technische omgeving van de AIVD en de MIVD de feitelijke gegevensverwerking in kaart brengen en beoordelen. Deze vorm van toezicht door de CTIVD is nieuw en zal de komende tijd, mede op basis van steekproeven, verder worden vormgegeven. Het gaat daarbij onder meer om de beoordeling van de werking van autorisaties, de status van databestanden (herkomst en eigenaarschap van data, tijdige vernietiging etc.), het combineren van gegevens en de toepassing van bestaande software of programmeertaal voor gegevensanalyse. De werking van door de diensten gebruikte algoritmes en modellen maakt hier onderdeel van uit.

De ICT Unit van de CTIVD zal de komende tijd investeren in het nader in kaart brengen van de ICT infrastructuur van de beide diensten en de technische omgeving waarbinnen de gegevensverwerking plaatsvindt. Hierin kunnen drie grotere deelgebieden worden onderkend: 1) het IT-landschap van de AIVD; 2) het IT-landschap van de MIVD; en 3) de omgeving van de Joint Sigint Cyber Unit (JSCU). Deze laatstgenoemde infrastructuur is onderdeel van het IT-landschap van de AIVD, maar vormt een separaat 'derde landschap' doordat de beide diensten samen verantwoordelijk zijn voor de gegevensverwerking die binnen de JSCU plaatsvindt. Continu onderzoek door de ICT Unit is van belang gelet op het dynamische karakter van de ICT ontwikkelingen en de rol van de techniek in het rechtmatig handelen van de diensten. De CTIVD verwacht hiermee een belangrijk fundament te leggen voor het blijvend effectief kunnen toetsen van de rechtmatigheid en kwaliteit van de gegevensverwerking door de AIVD en de MIVD.

De steekproeven naar datareductie en geautomatiseerde data-analyse zijn eind augustus 2019 gestart. Door de complexiteit en diversiteit aan systemen is de steekproef naar datareductie nog niet afgerond. De CTIVD geeft in paragraaf 3.2 een eerste beeld van haar bevindingen. De komende tijd zal de steekproef voortgezet worden. De resultaten hiervan worden in de vierde voortgangsrapportage op hoofdlijnen uiteengezet. De steekproef naar geautomatiseerde data-analyse betreft een vervolg op een eerdere steekproef die in het najaar van 2018 is verricht. De CTIVD zal begin 2020 een derde streekproef naar geautomatiseerde data-analyse verrichten.

In het algemeen kwam uit de verrichte steekproeven het beeld naar voren dat de AIVD en de MIVD beschikken over professionele, gedreven technisch specialisten, die met soms beperkte mogelijkheden onder aanzienlijke tijdsdruk diverse en complexe systemen hebben aangepast en ingericht om aan de nieuwe vereisten van de Wiv 2017 te voldoen. Er is een duidelijk verschil zichtbaar tussen de ICT-infrastructuur van de AIVD respectievelijk de JSCU en de ICT-infrastructuur van de MIVD. De MIVD heeft een achterstand in de IT-systemen. Dit heeft er ook voor gezorgd dat de ICT Unit van de CTIVD niet met dezelfde diepgang technisch onderzoek heeft kunnen verrichten bij de MIVD.

## 3.2 Steekproef datareductie

**Achtergrond**

Een essentieel onderdeel van datareductie is de wettelijke verplichting van de AIVD en de MIVD om gegevens afkomstig uit de inzet van bijzondere bevoegdheden zo spoedig mogelijk op relevantie te beoordelen. Gegevens die niet-relevant zijn beoordeeld dan wel waarvan de wettelijke bewaartermijn

is verstreken, moeten terstond worden vernietigd (artikel 27 Wiv 2017). Beide diensten hebben een systeem opgezet dat hier invulling aan moet geven. De wijze waarop dit gebeurt, verschilt echter aanzienlijk. Dit heeft te maken met het eerder genoemde kwaliteitsverschil tussen de IT-landschappen van de AIVD en de MIVD.

Gegevens die door de diensten worden verzameld door de inzet van bijzondere bevoegdheden, worden voorzien van een set aanvullende gegevens (labels). Labels bevatten bijvoorbeeld een datum en tijdgroep van het verwerven, de oorsprong van de gegevens en de bevoegdheid waarmee de gegevens verworven zijn. Labelmanagers scannen regelmatig de verzamelde gegevens, per systeem waarin die gegevens worden verwerkt. Indien nodig passen zij labels aan of voegen zij aanvullende labels toe. Het gaat hier in ieder geval om labels die de status van de relevantiebeoordeling aangeven (bijvoorbeeld relevant bevonden, relevantie nog onbekend, niet relevant). Zij maken daarbij gebruik van een database gevuld met (technische) kenmerken, zoals emailadressen of telefoonnummers. De wijze waarop dit plaatsvindt is bijzonder complex en is mede afhankelijk van de aard van de gegevens en het desbetreffende verwerkingssysteem. Vanwege deze complexiteit heeft de ICT Unit van de CTIVD de steekproef naar datareductie nog niet afgerond, maar geeft hieronder een beeld van haar voorlopige bevindingen.

### Voorlopige bevindingen AIVD

De AIVD heeft op hoofdlijnen een goed doordachte datareductie systematiek ontwikkeld dat grotendeels geautomatiseerd plaatsvindt en onder meer wordt uitgevoerd door labelmanagers. Het expliciet of impliciet relevant verklaren van gegevens wordt technisch ondersteund door de verwerkingssystemen. Niet-relevant beoordeelde gegevens worden veelal geautomatiseerd vernietigd. Daarnaast zijn er aanvullende procedurele maatregelen die zien op datareductie en die medewerkers richtlijnen geven in de dagelijkse omgang met het verwerken van gegevens.

De ICT Unit heeft de voorlopige indruk dat het datareductie beleid van de AIVD en de vertaling daarvan naar oplossingen in de techniek op onderdelen nog onvoldoende op elkaar aansluiten. Het datareductie systeem van de AIVD heeft zich door de tijd ontwikkeld en de ontwikkeling van de verschillende daaraan gerelateerde applicaties heeft grotendeels decentraal in de organisatie plaatsgevonden. Hoewel er een zekere mate van centrale sturing plaatsvond, lijkt veel vrijheid te zijn geboden aan ontwikkelaars oplossingen te zoeken en systemen in te richten. Mede als gevolg hiervan is het datareductie stelsel divers en complex en lijkt adequate interne controle vooralsnog moeilijk te realiseren. De ICT Unit zal dit verder in kaart brengen bij de voortzetting van de steekproef.

### Voorlopige bevindingen MIVD

Bij de MIVD is de systematiek van datareductie hoofdzakelijk procedureel van aard, waarbij op onderdelen technische ondersteuning wordt geboden. Dit brengt hogere risico's op onrechtmatigheden met zich mee omdat sneller sprake kan zijn van menselijke fouten. Veranderingen zijn reeds ingezet door de MIVD, maar structurele verbeteringen zijn pas op de langere termijn voorzien. Voor het Sigint-verwerkingssysteem heeft de MIVD wel mogelijkheden het proces van vernietiging na relevantiebeoordeling geautomatiseerd plaats te laten vinden. Dit is echter nog niet in de operationele omgeving doorgevoerd.

Medewerkers van de MIVD maken in het kader van de gemeenschappelijk JSCU ook gebruik van verwerkingssystemen van de AIVD. Hierdoor is sprake van een verplichting tot datareductie voor de MIVD ten aanzien van deze gegevens binnen de IT-infrastructuur van de AIVD/JSCU. Bij de beoordeling van de relevantie van gegevens is het voor MIVD medewerkers van belang gebruik te kunnen maken van de al opgebouwde kennis in lopende onderzoeken, die binnen de MIVD-infrastructuur beschikbaar is. De AIVD en de MIVD hebben samen een technische mogelijkheid gevonden om verantwoord verbinding te leggen tussen de beide netwerken. Het ontbreekt echter nog aan een synchronisatie op basis waarvan de status van gegevens, die deels ook op het netwerk van de MIVD aanwezig kunnen

zijn, automatisch worden aangepast aan de nieuwe status als gevolg van de relevantiebeoordeling op het netwerk van de AIVD/JSCU. Hierdoor is het risico aanwezig dat gegevens op de systemen van de MIVD nog aanwezig zijn, terwijl deze door de MIVD reeds zijn verwijderd op het systeem van de AIVD.

Een ander risico dat zich voordoet bij de MIVD ontstaat bij het doorzetten van nog niet op relevantie beoordeelde gegevens via een bepaalde verbinding naar het netwerk van de AIVD/JSCU, waar MIVD medewerkers deze gegevens verder verwerken. Omdat er sprake is van een kopie-houdend systeem, blijven de originele gegevens opgeslagen op het systeem bij de MIVD. Door het ontbreken van synchronisatie worden de gegevens alleen op de locatie bij de AIVD op relevantie onderzocht en in voorkomend geval vernietigd, terwijl de gegevens in ieder geval tot aan het einde van de bewaartermijn in zijn geheel op het systeem van de MIVD blijven staan.

#### Voorlopige bevindingen AIVD en MIVD

Uit de steekproef komt verder naar voren dat het technisch mogelijk is gegevens aan de verwerkingssystemen te onttrekken en bijvoorbeeld op een harde schijf op te slaan of te e-mailen binnen of tussen de beide diensten. In dergelijke gevallen kunnen gegevens op plekken terechtkomen die niet direct zichtbaar zijn en is sprake van een onderbroken *data lineage* (herkomst en verloop van data). Het risico bestaat bovendien dat niet relevante gegevens ten onrechte bewaard blijven. Hoewel er veel werk is verzet om ook oude data verzameld op basis van de Wiv 2002 te verwijderen uit deze omgevingen, is er nog geen gestructureerde controle binnen de AIVD en de MIVD op dit vlak. Het probleem wordt echter wel door beide diensten onderkend.

## 3.3 Steekproef geautomatiseerde data-analyse

#### Achtergrond

De ICT Unit van de CTIVD heeft een tweede steekproef uitgevoerd naar geautomatiseerde data-analyse ex. artikel 50 Wiv 2017 (ook wel metadata-analyse in het kader van onderzoeksopdrachtgerichte interceptie). De eerste steekproef vond plaats in oktober en november 2018. De steekproef beoogde twee vragen te beantwoorden:

1. Is sprake van risico's of indicaties dat de door de diensten verrichte metadata-analyse onrechtmatig plaatsvindt (d.w.z. zonder een daartoe verleende toestemming)?
2. Kan de CTIVD effectief toezien op de toepassing van metadata-analyse?

Om ten behoeve van adequate interne controle en effectief extern toezicht risico's op een onrechtmatige toepassing van deze bevoegdheid te kunnen onderkennen, zijn onderliggende gegevens nodig. Het gaat hierbij onder meer om loggegevens van de analysehandelingen die zijn verricht en om referentiegegevens op basis waarvan een nadere duiding kan plaatsvinden. Aan de hand van deze onderliggende gegevens moet antwoord kunnen worden gegeven op de volgende vragen:

- Welke vorm van geautomatiseerde data-analyse wordt toegepast en is deze gericht op het identificeren van personen of organisaties?
- Wordt er metadata uit onderzoeksopdrachtgerichte interceptie betrokken?
- Valt de verrichte geautomatiseerde data-analyse onder een goedgekeurd verzoek tot toestemming, waaronder onder meer het moment van de activiteit, het onderzoek waarbinnen het plaatsvindt, de medewerker die de activiteit verricht heeft, de andere gegevenssets die zijn betrokken, en de analysevorm die is toegepast?

Er dient in ieder geval (grotendeels) geautomatiseerd te kunnen worden nagegaan of een verrichte analysehandeling valt binnen de reikwijdte van een verleende toestemming. Op deze wijze kunnen

(risico's op) onrechtmatigheden worden geconstateerd. Vervolgens kunnen voor zover nodig mitigerende maatregelen worden genomen.

Bij de eerste steekproef in oktober en november 2018 is onderzoek gedaan naar de toepassing van metadata-analyse op het data platform van de AIVD met behulp van een drietal applicaties, waarvan ook de MIVD gebruik maakt. De CTIVD had logbestanden opgevraagd van drie applicaties. Dit betrof een zoek-applicatie, een netwerkanalyse-applicatie en een applicatie om query's (SQL) uit te kunnen voeren. Na analyse van deze logbestanden stelde de CTIVD vast dat niet (geautomatiseerd) is na te gaan of metadata-analyse al dan niet rechtmatig heeft plaatsgevonden en dat daarmee adequate interne controle en effectief extern toezicht dan ook niet mogelijk zijn. Naar aanleiding van de steekproef hebben gesprekken plaatsgevonden met de AIVD en de MIVD over de inrichting van een intern controlemechanisme, wat ook de CTIVD in staat moet stellen effectief toezicht uit te oefenen. Zo is onder meer gesproken over de aanpassing van loggegevens en het gebruik van dashboards of geautomatiseerde management rapportages van de data-analyse die heeft plaatsgevonden.

De ICT Unit van de CTIVD heeft in september 2019 een tweede steekproef uitgevoerd en heeft hiertoe opnieuw logbestanden en referentiebestanden opgevraagd van applicaties op het AIVD netwerk, die ook door de MIVD worden gebruikt. Het betrof twee applicaties waarvan ten behoeve van de eerste steekproef ook logbestanden zijn opgevraagd (een netwerkanalyse applicatie en een applicatie om query's uit te voeren) en vier applicaties die nog niet eerder waren beoordeeld. De ICT Unit is bij het onderzoek goed gefaciliteerd door medewerkers van de AIVD, in het bijzonder door de technisch specialisten en het 'CIO office'. Naast applicaties die door zowel de AIVD als MIVD gebruikt worden, is gekeken naar de vastlegging van het gebruik van een applicatie van de MIVD, waarmee toegang verkregen kan worden tot data uit onderzoeksopdrachtgerichte interceptie.

### Logbestanden

De logbestanden van de AIVD en/of de MIVD met betrekking tot de onderzochte analyse applicaties zijn onvolledig.

*Eerder onderzochte applicaties*

De vastlegging van het gebruik van een netwerk-analyseapplicatie die in de eerste steekproef ook is meegenomen, is verbeterd door enerzijds de verrichte handelingen in logbestanden te documenteren en door vast te leggen uit welke bronnen (datasets en toegepaste bevoegdheid) een resultaat van een geautomatiseerde data-analyse voortkomt. Uit de logbestanden blijkt echter niet welke gegevens zijn betrokken in de analysehandeling (of er bepaalde filters zijn toegepast of specifiek bepaalde datasets zijn geselecteerd). Bovendien is in een beperkt aantal gevallen niet te herleiden welke medewerker de analysehandeling uitvoert. In een andere al eerder beoordeelde applicatie die gebruikt wordt om SQL toe te passen, zijn geen wijzigingen aangebracht in wat wel en niet wordt gelogd. In enkele gevallen is de uitgevoerde query niet geheel vastgelegd.

*Nieuw onderzochte applicaties*

Binnen twee applicaties, die het mogelijk maken om vrijwel elke vorm van geautomatiseerde data-analyse toe te passen op de voor de medewerker beschikbare datasets, worden handelingen niet gelogd of vastgelegd. Een volledig overzicht van medewerkers die deze applicaties kunnen gebruiken is evenmin beschikbaar. Van twee zoek-applicaties is geen informatie beschikbaar om de logbestanden te kunnen duiden. In één van de applicaties is niet te herleiden welke datasets bij de GDA zijn betrokken en in beide applicaties wordt niet vastgelegd of de resultaten gegevens uit onderzoeksopdrachtgerichte interceptie bevatten.

De applicatie die bij de MIVD veel gebruikt wordt om gegevens uit onderzoeksopdrachtgerichte interceptie te verwerken, bevat een audit-functionaliteit. Deze functionaliteit wordt weliswaar nog niet gebruikt ten behoeve van interne controle, maar vormt hiervoor wel een goede basis.

### Referentiebestanden

Ook de referentiebestanden van de beide diensten bieden nog niet alle benodigde gegevens. Risico's op een onrechtmatige toepassing van geautomatiseerde data-analyse hangen samen met de mate waarin medewerkers in operationele teams analyse applicaties kunnen gebruiken en toegang hebben tot metadata uit onderzoeksopdrachtgerichte interceptie. Om risico's in kaart te brengen is dus een overzicht nodig van welke datasets afkomstig zijn uit onderzoeksopdrachtgerichte interceptie, welke medewerkers toegang hebben tot welke datasets en tot welke analyse applicaties medewerkers toegang hebben. Deze referentiebestanden waren op navraag niet beschikbaar. Wel is door de AIVD een bestand aangeleverd waarin is opgenomen in welke teams welke medewerkers op dat moment actief waren. Dit bestand is niet volledig, kent geen historie en evenmin een koppeling tot verleende toestemming voor de toepassing van geautomatiseerde data-analyse.

Met betrekking tot de beoordeelde MIVD applicatie zijn de nodige referentiebestanden beschikbaar in de applicatie. Het gaat om informatie over welke medewerkers in welke teams toegang hebben tot de applicatie en tot de onderliggende gegevens, op basis van welke verleende toestemming. Deze referentiegegevens zijn alleen bruikbaar ten behoeve van controle op het gebruik van deze specifieke applicatie.

### Bevindingen AIVD en MIVD

De ICT Unit heeft op basis van de beperkt beschikbare gegevens herleid of er indicaties zijn dat de door de diensten verrichte geautomatiseerde data-analyse onrechtmatig plaatsvindt. Uit het combineren van de logbestanden en referentiebestanden van één bepaalde applicatie kan worden geconcludeerd dat enkele AIVD- en MIVD-medewerkers die actief waren in een operationeel team gebruik hebben gemaakt van een netwerkanalyseapplicatie, waarbij zij metadata uit onderzoeksopdrachtgerichte interceptie hebben betrokken. Dit was niet te relateren aan een goedgekeurd verzoek tot toestemming in die periode en is daarmee onrechtmatig. Inmiddels heeft de AIVD ook zelf vastgesteld dat onrechtmatige geautomatiseerde data-analyse heeft plaatsgevonden en is door de dienst nader onderzoek ingesteld.

Een adequaat intern controlemechanisme gericht op de rechtmatige toepassing van geautomatiseerde data-analyse is bij de diensten nog niet in gebruik. Er wordt op dit moment bij de AIVD een applicatie ontwikkeld die een sluitende administratie met referentiegegevens tot stand kan brengen. Ook de MIVD is bij de ontwikkeling van de applicatie betrokken. Het betreft onder meer gegevens die het mogelijk kunnen maken om goedgekeurde verzoeken tot toestemming voor geautomatiseerde data-analyse ex. artikel 50 Wiv 2017 te koppelen aan onderzoeken, teams en medewerkers van beide diensten. Hoewel er nu meer gegevens beschikbaar zijn dan ten tijde van de steekproef in het najaar van 2018, zijn adequate interne controle en effectief extern toezicht op de toepassing van geautomatiseerde data-analyse ex. artikel 50 van de Wiv 2017 nog niet mogelijk.

# 4 Vervolg

## Voortgangsrapportages

De toezichtsactiviteiten naar de invoering van de Wiv 2017 vinden in ieder geval tot mei 2020 plaats. Met het oog op de vervroegde evaluatie van de Wiv 2017, waarvan de start voor mei 2020 is beoogd, streeft de CTIVD er nadrukkelijk naar binnen twee jaar na de inwerkingtreding van de wet in concluderende zin te rapporteren over de onderwerpen die zijn geduid tijdens de parlementaire behandeling van de wet en aan de CTIVD voor onderzoek zijn voorgelegd.[2] Zij rapporteert ten minste halfjaarlijks aan de betrokken ministers en het parlement. De vierde en laatste voortgangsrapportage wordt vastgesteld in mei 2020.

## Nulmetingen

*Nulmeting OOG interceptie kabel*

De AIVD en de MIVD zijn nog volop bezig met het operationaliseren van de onderzoeksopdrachtgerichte interceptie van de kabel. Het is daarom nog steeds te vroeg ten aanzien hiervan een nulmeting te verrichten. De CTIVD is zich in dat verband blijven richten op de inzet van onderzoeksopdrachtgerichte interceptie van de ether. Zodra onderzoeksopdrachtgerichte interceptie van de kabel is geoperationaliseerd, zal de CTIVD een nulmeting verrichten naar de feitelijke toepassing van wettelijke waarborgen daarbij. De CTIVD heeft niet de verwachting in de vierde en laatste voortgangsrapportage een (sluitend) beeld te kunnen schetsen hoe onderzoeksopdrachtgerichte interceptie van de kabel in de praktijk wordt toegepast en op welke wijze de rechtsbescherming van de burger in dat verband wordt gewaarborgd. Wel zal zij, mede op basis van de toetsing van de resultaten van het verbeterprogramma voor onderzoeksopdrachtgerichte interceptie (zie paragraaf 2.4), een indicatie van de aanwezige risico's kunnen geven.

## Steekproeven

*Steekproef naar de werking van het datareductie systeem*

De CTIVD heeft in het najaar van 2019 een start gemaakt met een (technische) steekproef naar de werking van het datareductie systeem. Vanwege de complexiteit hiervan en een veelheid aan technische systemen waarmee de diensten werken, heeft de steekproef vooralsnog slechts voorlopige bevindingen opgeleverd (zie paragraaf 3.2). De steekproef zal het komend half jaar worden gecontinueerd. De resultaten hiervan worden besproken in de laatste voortgangsrapportage.

*Steekproef naar geautomatiseerde metadata-analyse ex. artikel 50*

De CTIVD zal begin 2020 een derde steekproef verrichten naar de toepassing van geautomatiseerde metadata-analyse ex. artikel 50 Wiv 2017 en de werking van een adequaat intern controle mechanisme (zie paragraaf 3.3). Centraal daarbij staat ook de vraag of de CTIVD effectief toezicht kan uitoefenen op de toepassing van deze bevoegdheid door de diensten.

*Steekproef naar geautomatiseerde data-analyse (GDA) ex. artikel 60*

In de tweede voortgangsrapportage heeft de CTIVD op basis van een nulmeting vastgesteld dat sprake is van overwegend hoge risico's op onrechtmatig handelen bij geautomatiseerde data-analyse die plaatsvindt op basis van artikel 60 Wiv 2017. Een steekproef naar de toepassing hiervan in de praktijk is dan ook van belang. Dit betreft een aanvulling op de eerdere nulmeting die zich heeft gericht op het beleid en de werkinstructies van de beide diensten. De CTIVD beoogt deze steekproef eveneens begin 2020 te starten.

2 Verzoek minister BZK i.v.m. moties en toezeggingen Wiv 2017, d.d. 25 april 2018, *Kamerstukken II* 2017/18, 34588 nr. 1 (bijlage).

## Diepteonderzoeken

*Onderzoek naar bulkhacks*

De inzet van de hackbevoegdheid maakt van het bredere thema van bulkverwerking door de AIVD en de MIVD een belangrijk onderdeel uit. In het onderzoek naar bulkhacks komt de vraag aan de orde of sprake is van voldoende waarborgen bij de inzet en toepassing van hacks waarmee een grote hoeveelheid gegevens (bulkdataset) kan worden verworven. Het gaat hierbij om gegevens waarvan het merendeel betrekking heeft op organisaties en/of personen die geen onderwerp van onderzoek van de diensten zijn en dat ook nooit zullen worden. Het onderzoek is bovendien van belang met het oog op de evaluatie van de Wiv 2017 die in mei 2020 zijn aanvang dient te krijgen. Het onderzoek naar bulkhacks is in september 2019 gestart.

*Onderzoek naar reisgegevens*

Een tweede onderwerp binnen het thema bulkverwerking door de AIVD en de MIVD betreft de inzet van de algemene bevoegdheid van de diensten in het kader waarvan eveneens grote hoeveelheden gegevens kunnen worden verworven. Het onderzoek is eind september 2019 van start gegaan en richt zich op de vraag of voldoende waarborgen aan de orde zijn bij de verwerving van grote hoeveelheden passagiersgegevens van luchtvaartmaatschappijen op basis van de algemene bevoegdheid van de diensten. Ook wordt aandacht besteed aan de verwerking en verstrekking van deze gegevens door de AIVD en de MIVD.

*Onderzoek naar de inzet van bijzondere bevoegdheden ter ondersteuning van de taakuitvoering*

In artikel 28 lid 2 Wiv 2017 is een nieuwe regeling opgenomen voor de inzet van bijzondere bevoegdheden *ter ondersteuning van de taakuitvoering*. Dit is toegestaan in twee specifieke gevallen: om te beoordelen of het nodig is om bijzondere veiligheidsmaatregelen te treffen voor een persoon die werkzaamheden voor de diensten verricht en om te beoordelen of personen, met wier hulp gegevens worden verzameld, betrouwbaar zijn. Als de betrokken minister toestemming geeft voor de inzet van een bijzondere bevoegdheid ter ondersteuning van de taaktuitvoering, dient de CTIVD daarvan terstond op de hoogte te worden gesteld. De CTIVD heeft het onderzoek begin oktober 2019 aangekondigd.

*Onderzoek naar overige wegingsnotities van de AIVD en de MIVD*

De CTIVD heeft in februari 2019 toezichtsrapport nr. 60 gepubliceerd over de wegingsnotities van de AIVD en de MIVD voor de internationale samenwerking met de Counter Terrorism Group- en sigint-partners. De aanbevelingen uit rapport nr. 60 zijn door de betrokken ministers overgenomen. Zij gaven daarbij aan dat de herziening van de onderzochte wegingsnotities uiterlijk 1 juli 2019 zou zijn afgerond. De wegingsnotities voor alle overige buitenlandse diensten waarmee een samenwerkingsrelatie bestaat, die op 1 januari 2019 gereed zouden zijn, dienden aan de hand van de aanbevelingen van rapport nr. 60 eveneens aangepast te worden. Het voltooien hiervan is voor de AIVD nu voorzien in 2021. Voor de MIVD is dit nog onduidelijk. Het heeft vooralsnog geen toegevoegde waarde nu een onderzoek naar al deze wegingsnotities te verrichten. De CTIVD is voornemens het onderzoek daarom in delen uit te voeren, afhankelijk van de snelheid waarmee de diensten de wegingsnotities aanpassen.

*Onderzoek naar samenwerkingsactiviteiten in de praktijk*

Wegingsnotities zijn in de kern een schriftelijke verantwoording van de beslissing binnen een bepaalde bandbreedte met een buitenlandse dienst samen te werken. De CTIVD zal onderzoek verrichten naar de werking hiervan in de praktijk. Daarbij staat de vraag centraal of de AIVD en de MIVD binnen de grenzen van de wegingsnotities blijven bij concrete samenwerkingsactiviteiten, zoals de uitwisseling van persoonsgegevens aan risicodiensten, en of deze samenwerkingsactiviteiten overigens voldoen aan de vereisten van de Wiv 2017. De CTIVD voorziet een start van dit onderzoek eind 2019.

Oranjestraat 15, 2514 JB Den Haag
Postbus 85556, 2508 CG Den Haag

**T** 070 315 58 20
**E** info@ctivd.nl | www.ctivd.nl