Bijlage bij de tweede Voortgangsrapportage

De werking van de Wiv 2017

CTIVD nr. 62

[vastgesteld op 14 mei 2019]

Commissie van Toezicht
op de Inlichtingen- en
Veiligheidsdiensten

Commissie van Toezicht
op de Inlichtingen- en
Veiligheidsdiensten

CTIVD nr. 62

BIJLAGE
VOORTGANGSRAPPORTAGE II

De werking van de Wiv 2017

Inhoudsopgave

Commissie van Toezicht
op de Inlichtingen- en
Veiligheidsdiensten

CTIVD nr. 62

BIJLAGE VOORTGANGSRAPPORTAGE II

De werking van de Wiv 2017

1 Methodiek

De AIVD en de MIVD hebben naar aanleiding van de eerste voortgangsrapportage van december 2018 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. De CTIVD heeft de activiteiten van de Wiv boards van de beide diensten op de voet gevolgd en heeft met regelmaat reflectie daarop gegeven. De concrete stappen die de beide diensten hebben gezet, worden benoemd in de tweede voortgangsrapportage en worden nader toegelicht in de hoofdstukken 2 t/m 4 van deze bijlage.

De CTIVD hanteert in haar voortgangsrapportages verschillende risico categorieën:

- **Geen risico**: Er wordt voldoende uitwerking gegeven aan het wettelijke kader en er zijn geen tekortkomingen in beleid, processen of in de toepassing daarvan vastgesteld. Het beleid is bovendien actueel.
- **Beperkt risico**: Er wordt voldoende uitwerking gegeven aan het wettelijke kader maar er zijn wel tekortkomingen in beleid, werkprocessen, systemen of in de toepassing daarvan vastgesteld. De tekortkomingen zijn van beperkte inhoudelijke of procedurele aard en zijn goed herstelbaar.
- **Gemiddeld risico**: Er wordt onvoldoende uitwerking gegeven aan het wettelijke kader doordat sprake is van inhoudelijke tekortkomingen in beleid, werkprocessen, systemen of in de toepassing daarvan. De tekortkomingen kunnen leiden tot onrechtmatig handelen van de diensten.
- **Hoog risico**: Er wordt onvoldoende uitwerking gegeven aan het wettelijke kader doordat beleid of processen geheel ontbreken of in strijd zijn met de wet, of doordat sprake is van onrechtmatigheden in de toepassing daarvan.

De CTIVD heeft de afgelopen maanden diepteonderzoeken verricht naar enkele onderdelen van het stelsel van onderzoeksopdrachtgerichte interceptie waar zij een hoog risico voor onrechtmatig handelen constateerde in haar eerste voortgangsrapportage. Deze diepteonderzoeken zien op de werking van filters waarmee een zo gericht mogelijke verwerving van gegevens dient te worden gerealiseerd en op de zo gericht mogelijke verwerking van gegevens bij de inzet van de selectiebevoegdheid. De bevoegdheid van selectie houdt in het kennis kunnen nemen van de inhoud van de onderschepte communicatie en deze inhoud op relevantie te beoordelen. Zowel filtering als selectie dragen bij aan de verantwoorde databeperking die binnen het stelsel van onderzoeksopdrachtgerichte interceptie aan de orde moet zijn. De resultaten van deze diepteonderzoeken zullen in de loop van 2019 worden gepubliceerd in separate toezichtsrapporten. Daarin staat centraal of de geconstateerde risico's uit de eerste voortgangsrapportage zich daadwerkelijk hebben gemanifesteerd in de praktijk. In deze

tweede voortgangsrapportage wordt uitsluitend besproken welke aanpassingen de beide diensten hebben gedaan in hun intern beleid, werkprocessen, de inrichting van technische systemen en hun interne controle mechanismen teneinde de risico's tegen te gaan.

Er is een steekproef uitgevoerd naar de toepassing van de bijzondere bevoegdheid van metadata-analyse ex. artikel 50 Wiv 2017. Deze steekproef was erop gericht vast te stellen of metadata-analyse binnen het stelsel van onderzoeksopdrachtgerichte interceptie conform de wettelijke regeling plaatsvindt respectievelijk of de CTIVD effectief toezicht daarop kan uitoefenen. Het wettelijk kader voor metadata-analyse ex. artikel 50 Wiv 2017 is onderwerp geweest van rechtseenheidoverleg tussen de Toetsingscommissie Inzet Bevoegdheden (TIB) en de CTIVD en heeft geleid tot veelvuldig overleg met zowel de departementen van Binnenlandse Zaken en Koninkrijksrelaties (BZK) en van Defensie als de AIVD en de MIVD. De problematiek van metadata-analyse is uitgelicht in hoofdstuk 5 van deze bijlage.

De CTIVD heeft een nulmeting verricht naar de inzet van de algemene bevoegdheid van geautomatiseerde data-analyse ex. artikel 60 Wiv 2017 in het reguliere inlichtingproces van de beide diensten. De uitkomst van deze nulmeting is een risico-inschatting. Het brengt in kaart waar risico's aanwezig zijn voor onrechtmatig handelen van de diensten en geeft de CTIVD richting voor het bepalen van haar verdere toezichtsactiviteiten. De nulmeting naar geautomatiseerde data-analyse ex. artikel 60 Wiv 2017 is verricht in de periode januari tot en met maart 2019 en wordt besproken in de tweede voortgangsrapportage.

De samenwerking met buitenlandse diensten, waaronder het bestaan en de inhoud van wegingsnotities en de uitwisseling van ongeëvalueerde gegevens is respectievelijk wordt onderzocht in een tweetal diepteonderzoeken. Het toezichtsrapport over de wegingsnotities van de AIVD en de MIVD voor de internationale samenwerking binnen de Counter Terrorism Group en met sigint-partners is reeds gepubliceerd. Het toezichtsrapport over de verstrekking van ongeëvalueerde gegevens aan buitenlandse diensten verschijnt in de loop van 2019. In deze tweede voortgangsrapportage wordt uitsluitend ingegaan op de wettelijke regeling voor dergelijke verstrekkingen door de AIVD en de MIVD en de wijze waarop dit een nadere invulling heeft gekregen in beleid en werkinstructies van de beide diensten. De toetsing van de praktijk komt aan de orde in het toezichtsrapport.

2 Zorgplicht

Essentie wettelijke regeling zorgplicht

De zorgplicht van de AIVD en de MIVD voor een rechtmatige gegevensverwerking is een essentiële waarborg voor zowel de gegevensbescherming als het toezicht daarop. Het houdt in dat de beide diensten voortdurend controle hebben op de wijze waarop zij gegevens verwerken en dat zij er zorg voor dragen dat de gegevensverwerking in overeenstemming is en blijft met de daarvoor geldende wettelijke voorschriften (*compliance*). Voortdurend in controle zijn vereist ook dat de diensten instrumenten gebruiken 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. Zonder dergelijke instrumenten, zonder een heldere structuur voor de zorgplicht, is het niet goed mogelijk voldoende interne controle uit te oefenen over de gegevensverwerking en is effectief extern toezicht daarop niet aan de orde.

Effectief toezicht houdt in dat de CTIVD doelgericht zicht kan hebben op elk proces van gegevensverwerking van de AIVD en de MIVD, zowel in de inrichting, toepassing als de resultaten daarvan. Het hebben van onbeperkte toegang tot gegevens alleen is daarbij niet voldoende. Dit zou betekenen dat de CTIVD zelf gegeven per gegeven handmatig moet beoordelen en haar capaciteit in personele zin disproportioneel moet uitbreiden om hiertoe in staat te zijn. Dat is haalbaar noch gewenst. Er moet sprake zijn van interne controle mechanismen op de gegevensverwerking bij de beide diensten, waartoe de wet verplicht en waar de CTIVD zich in haar toezicht mede op kan baseren.

Eerder vastgestelde risico's

De CTIVD heeft in haar eerste voortgangsrapportage geconstateerd dat er geen instrumentarium voor de zorgplicht aanwezig was bij de AIVD en de MIVD. Het ontbreken van een doorlopende interne controle op de gegevensverwerking door de diensten zelf vormde een rode draad in de resultaten van de destijds door de CTIVD verrichte nulmetingen. De CTIVD karakteriseerde het risico op onrechtmatige gegevensverwerking door de beide diensten als hoog. Zij vond het van essentieel belang dat het instrumentarium voor de zorgplicht op een zo kort mogelijke termijn concreet wordt ingericht en geïmplementeerd. Dit vraagt om een tijdsplanning waaruit het belang van de zorgplicht blijkt.

Toezeggingen

In hun reactie op de eerste voortgangsrapportage hebben de beide ministers onder meer aangegeven dat een werkprogramma voor de zorgplicht in het eerste kwartaal van 2019 gereed is. Dit omvat ook het uitwerken van een systematiek van interne controle, waaronder assessments en audits. Ook stelden de ministers dat bij de AIVD een portefeuillehouder zorgplicht en compliance is aangesteld om de naleving van de zorgplicht structureel te borgen en dat bij de MIVD een *chief information officer* wordt aangesteld en een *compliance office* wordt opgericht.[1] Verder is aangegeven dat monitoring van en controle op rechtmatige gegevensverwerking plaats dient te vinden. De beide diensten zullen in dit kader onder meer een aantal audits uitvoeren komend jaar.[2]

1 *Kamerstukken II* 2018/19, 34588 nr. 80.
2 *Kamerstukken II* 2018/19, 34588 nr. 81.

Voortgang AIVD

De AIVD heeft een kader voor de zorgplicht vastgesteld (maart 2009) langs de lijn van tien overkoepelende normen die voortvloeien uit de Wiv 2017. Deze normen omvatten de wettelijke vereisten waaraan de diensten moeten voldoen bij de verwerking van (persoons)gegevens. Door de AIVD te nemen passende maatregelen moeten zorgen voor naleving van de wet. Een passende maatregel moet volgens het kader voorzien in *data protection by design* en *by default*.[3]

De invulling en naleving van de tien normen wordt getoetst en gemonitord vanuit het algemeen bekende en breed toegepaste organisatiemodel van *Three Lines of Defense*. De AIVD is bezig met de inrichting van dit model en heeft daarin concrete stappen gezet. Het model gaat uit van een controlestructuur in drie organisatielijnen. Voor de derde lijn (onafhankelijke interne controle) is een auditinstrument vastgesteld (februari 2019), waarvan structureel gebruik zal worden gemaakt. Een eerste audit is uitgevoerd naar een onderdeel van de datareductie systematiek. De tweede lijn (risico en *compliance* management) wordt stapsgewijs ingericht over een langere termijn. De AIVD heeft een portefeuillehouder zorgplicht en compliance (als kwartiermaker) en enkele privacy experts aangesteld en heeft op de Wiv 2017 gerichte opleidingen in gang gezet. Ook is besloten in 2019 risicoanalyses uit te voeren op werkprocessen m.b.t. de inzet van (bijzondere) bevoegdheden. Er zijn inmiddels twee risicoanalyses verricht die betrekking hadden op gericht tappen en etherinterceptie door de AIVD. Voor de inrichting van de tweede lijn is in maart 2019 een goede opzet voor het komende jaar vormgegeven en door de dienstleiding vastgesteld. In de eerste lijn (het primaire, operationele proces) ligt de nadruk vooralsnog op het op een juiste wijze beleggen van verantwoordelijkheden. Hier is een begin mee gemaakt.

De AIVD is inmiddels doordrongen van de noodzaak van adequate interne controle op de naleving van de wet (*compliance*). In het afgelopen half jaar heeft de AIVD ook zelf moeten vaststellen dat de benodigde interne sturing en controle verbeterd dienden te worden ten aanzien van onderdelen van het stelsel van onderzoeksopdrachtgerichte interceptie van de ether.[4] Dit was zowel confronterend voor de dienst als een gelegenheid het zelflerend vermogen te laten zien. De AIVD heeft naar aanleiding hiervan op eigen initiatief besloten de onderzoeksopdrachtgerichte interceptie van de kabel pas in te zullen zetten nadat voldoende zeker is gesteld dat het interceptieproces werkt zoals het behoort te werken en de AIVD daarover voldoende controle heeft.

De implementatie van de zorgplicht door de AIVD is nu nog niet zo ver gevorderd dat de CTIVD de werking hiervan al in de breedte kan toetsen. De CTIVD zal de voortgang hiervan blijven volgen. De risico inschatting wordt voor de AIVD **bijgesteld van hoog naar beperkt**.

Voortgang MIVD

De MIVD heeft begin mei 2019 een (beleids)kader vastgesteld voor de invulling van de zorgplicht. De algemene beginselen van gegevensbescherming (waaronder *data protection by design* en *by default*) gelden hierbij als uitgangspunt voor het nemen van maatregelen.

Net als de AIVD heeft de MIVD besloten de inrichting van de zorgplicht te realiseren door toepassing van het organisatiemodel van *Three Lines of Defense*. De MIVD investeert eerst en vooral in het beter in kaart brengen en beschrijven van de eigen werkprocessen in de eerste lijn (het primaire proces), als basis voor het vervolgens aanbrengen van verbeteringen. Het doel hiervan is het inzichtelijk maken

3 *Data protection by design* houdt in dat gegevensbescherming bij de inrichting van processen en het ontwerp van applicaties en systemen wordt meegenomen en ingebouwd. *Data protection by default* is een verwant begrip. Het wil zeggen dat de standaardinstellingen in applicaties en systemen zodanig zijn ingesteld dat deze maximale gegevensbescherming bieden. Voor het aanpassen hiervan moeten gebruikers extra handelingen verrichten, waardoor het toepassen van een lager niveau van gegevensbescherming dan hetgeen de standaardinstellingen bieden steeds een bewuste handeling moet zijn.

4 Een nadere toelichting is opgenomen in hoofdstuk 4 van de bijlage.

van verantwoordelijkheden binnen de organisatie en eventuele tekortkomingen daarin. Ook heeft de MIVD op de Wiv 2017 gerichte opleidingen in gang gezet. Er is nog geen concrete aanpak voor de inrichting van de verdere interne controlestructuur uitgewerkt. De MIVD heeft besloten instrumenten als risicoanalyses en audits in te stellen, maar deze zijn nog niet geconcretiseerd.

De MIVD heeft concrete stappen gezet door de werving van gespecialiseerde functionarissen. Zo heeft de MIVD mede in het kader van de zorgplicht een *chief information officer* (CIO) geworven. Deze CIO is gezien de staat van de ICT-infrastructuur van groot belang voor het creëren van randvoorwaarden voor een gedegen interne controle binnen de MIVD. Ook is een *compliance officer* aangesteld en is een interne auditor geworven, die respectievelijk de tweede lijn (risico en *compliance* management) en de derde lijn (onafhankelijke interne controle) nader vorm moeten geven. Deze personen zijn in april 2019 in functie getreden.

De MIVD is medio april 2019 begonnen met een ICT-pilot gericht op het ontwikkelen van een moderne data architectuur. Hiermee wordt een start gemaakt met de modernisering van het MIVD ICT-landschap dat ook meer mogelijkheden zal bieden voor het technisch ondersteunen van interne controle. De herinrichting van het ICT-landschap is een meerjarig traject waarvan de einddatum nog niet is vastgesteld. In verband hiermee is de MIVD bezig met verschillende ICT-projecten die (moeten) voorzien in tussentijdse oplossingen. De MIVD maakt de keuze tussentijdse technische oplossingen zo veel mogelijk te richten naar de uiteindelijk beoogde data architectuur.

De risico inschatting wordt voor de MIVD **bijgesteld van hoog naar gemiddeld** in het licht ook dat de MIVD in het komende half jaar de genomen besluiten verder tot uitvoering zal brengen.

3 Datareductie

Essentie wettelijke regeling

De verplichting tot permanente datareductie vormt de hoeksteen van de privacybescherming in de Wiv 2017. Kortgezegd komt het erop neer dat de AIVD en de MIVD de gegevens die zij verzamelen door de inzet van bijzondere bevoegdheden, zoals gericht tappen, hacken, het opvragen van opgeslagen gegevens etc., zo spoedig mogelijk op relevantie moeten 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. Gegevens verzameld door onderzoeksopdrachtgerichte interceptie vallen buiten deze regeling. Daarvoor geldt een bewaartermijn van 3 jaar.

Om adequaat invulling te geven aan deze wettelijke plicht is een gedegen systematiek van datareductie vereist, die niet alleen zijn weerslag krijgt in het beleid, werkinstructies en de werkprocessen van de diensten, maar ook in technische zin goed is ingebed. De werking hiervan moet bovendien intern gecontroleerd worden en extern effectief toezicht door de CTIVD mogelijk maken. Dit laatste betekent dat het voor de CTIVD herleidbaar moet zijn op basis waarvan gegevens relevant zijn beoordeeld en toetsbaar moet zijn dat niet relevante gegevens terstond en niet beoordeelde gegevens tijdig zijn vernietigd. Een dergelijke systematiek van datareductie is bijzonder complex en niet eenvoudig te realiseren. Een goede ICT infrastructuur is daarbij cruciaal.

De verplichting tot datareductie kent enkele cruciale onderdelen die nadere invulling dienen te krijgen in het beleid, werkinstructies, processen en de inrichting van technische systemen van de diensten.

3.1 Wat wordt verstaan onder relevante gegevens en wat niet?

Eerder vastgestelde risico's

De diensten hanteren een ruime definitie voor relevantie. De CTIVD heeft hier, gelet op het belang daarvan voor het inlichtingenproces, begrip voor geuit. Zij vond het wel noodzakelijk dat aanvullend wordt gemotiveerd waarom gegevens relevant zijn beoordeeld, indien een objectieve beoordeling van de gegevens in redelijkheid niet direct leidt tot de conclusie dat deze relevant zijn. Dit diende in beleid te worden vastgelegd. De CTIVD beoordeelde het risico voor de beide diensten als beperkt.

Voortgang AIVD en MIVD

De AIVD heeft een nieuw beleidskader opgesteld. Dit beleid is helder en biedt concrete handvatten voor het (aanvullend) motiveren waarom op inhoud beoordeelde gegevens als relevant zijn aangemerkt. Het beleid dient nog een (technische) vertaalslag te krijgen in de applicaties die door medewerkers van de AVD gebruikt worden voor de verwerking van gegevens. De MIVD heeft het belang van een aanvullende motivering in voorkomende gevallen onderschreven, maar het beleid en werkwijze op dit punt nog niet aangepast. De risico inschatting wordt voor de beide diensten **gehandhaafd op beperkt**.

3.2 Welke beoordelingstermijn wordt gehanteerd?

Eerder vastgestelde risico's

In het inlichtingenproces ligt besloten dat de relevantiebeoordeling in veel gevallen binnen drie maanden plaatsvindt. Dit geldt echter niet altijd. Houvast over wat in welke gevallen moet worden verstaan onder het 'zo spoedig mogelijk' op relevantie beoordelen ontbrak nog in beleid en werkinstructies van de beide diensten, waardoor een verschuiving kan optreden van het moment van beoordeling. Belangrijk is ook dat nog niet was voorzien in een regeling voor het bepalen van de relevantie van nog niet beoordeelde data die onder de Wiv 2002 zijn verzameld, anders dan dat niet

beoordeelde 'oude data' op 1 mei 2019 vernietigd dienden te worden. De CTIVD constateerde dat sprake was van een gemiddeld risico voor de beide diensten.

Voortgang AIVD

De AIVD heeft in beleid en werkinstructies opgenomen wat wordt verstaan wordt onder het 'zo spoedig mogelijk' op relevantie beoordelen. Daarnaast is in beleid neergelegd onder welke omstandigheden de bewaartermijn van één jaar met een half jaar verlengd mag worden, conform de wettelijke regeling daarvoor.

Er is gewerkt aan de vernietiging van data die is verzameld onder de oude wet. Deze gegevens (voor zover niet verzameld met ongerichte interceptie onder de Wiv 2002) dienden voor 1 mei 2019 op relevantie beoordeeld of vernietigd te zijn. Een deel hiervan is reeds opgeschoond. Het resterende deel is nog niet beoordeeld op relevantie. Deze gegevens kunnen nog steeds noodzakelijk zijn voor de taakuitvoering van de dienst. Integrale vernietiging van het resterende deel zou voor de AIVD derhalve tot een operationeel risico leiden. De AIVD heeft in maart 2019 beleid opgesteld voor de relevantiebeoordeling van deze gegevens. Dit beleid was naar het oordeel van de CTIVD niet conform de wettelijke regeling voor datareductie. Het zou er onder meer toe leiden dat grote sets gegevens integraal als relevant worden aangemerkt zonder dat hier een juiste beoordeling aan ten grondslag ligt. De CTIVD heeft aangedrongen op afstemming met het ministerie van BZK, waaronder de directie Constitutionele Zaken en Wetgeving (CZW), over de rechtmatigheid van dit beleid.

Mede naar aanleiding van overleg met het departement heeft de AIVD in april 2019 besloten een andere route te bewandelen die wél in lijn is met de regeling in de Wiv 2017. De bewaartermijn van gegevens die zijn verzameld met bijzondere bevoegdheden (met uitzondering van ongerichte interceptie) is met een half jaar verlengd, hetgeen wettelijk is toegestaan. De minister van BZK is hierover geïnformeerd. Deze gegevens moeten nu voor 1 november 2019 relevant beoordeeld dan wel vernietigd zijn. De AIVD heeft het komend half jaar een grote uitdaging in het op relevantie beoordelen van deze Wiv 2002 gegevens. Het gaat om een aanzienlijke hoeveelheid gegevens. Het is de vraag of het de AIVD lukt de gegevens op relevantie te beoordelen binnen de termijn. De dienstleiding van de AIVD heeft aangegeven dat voor 1 november 2019 een structurele oplossing zal worden ingericht. Vervolgens zullen gegevens die als niet relevant zijn beoordeeld en gegevens die niet zijn beoordeeld worden vernietigd. Voor gegevens die op basis van de Wiv 2002 zijn verzameld met de toenmalige bevoegdheid van ongerichte interceptie geldt dat deze binnen drie jaar na de inwerkingtreding van de Wiv 2017 relevant beoordeeld of vernietigd moeten zijn. De termijn daarvoor verloopt op 1 mei 2021.

De AIVD heeft verder besloten, conform de wettelijke mogelijkheid daarvoor, de bewaartermijn voor een aantal bulkdatasets die vanaf 1 mei 2018 op basis van de Wiv 2017 zijn verkregen (o.a. door de inzet van de hackbevoegdheid) met een half jaar te verlengen. De relevantiebeoordeling van de desbetreffende gegevens is nog niet voltooid. De minister van BZK is hiervan op de hoogte gesteld.

Het risico voor het zo spoedig mogelijk op relevantie beoordelen van gegevens wordt voor de AIVD **bijgesteld van gemiddeld naar beperkt**. Het komende half jaar zal moeten uitwijzen of deze beoordeling gehandhaafd kan worden.

Voortgang MIVD

De MIVD heeft in maart 2019 beleid vastgesteld waarin wordt uitgelegd hoe een 'zo spoedig mogelijke' relevantiebeoordeling vorm dient te krijgen. Uitgangspunt is dat bij elke verlenging van een bijzondere bevoegdheid de gegevens op relevantie beoordeeld moeten zijn (doorgaans binnen drie maanden). In het beleid is aangegeven onder welke omstandigheden de beoordeling meer tijd mag innemen. Om te voorkomen dat het moment 'zo spoedig mogelijk' structureel vlak voor het einde van de bewaartermijn komt te liggen, zullen beoordelaars elke drie maanden een automatische herinnering ontvangen van de nog op relevantie te beoordelen data. De ICT-ondersteuning hiervoor is echter nog niet gereed.

De MIVD heeft ernaar gestreefd alle gegevens die zijn verzameld op basis van de Wiv 2002, met uitzondering van gegevens afkomstig uit ongerichte etherinterceptie, vóór 1 mei 2019 relevant te beoordelen dan wel te vernietigen conform de wettelijke regeling. De MIVD heeft onder meer per verwerkingssysteem in kaart gebracht wat er nodig is om gegevens op relevantie te kunnen beoordelen Voor de meeste verwerkingssystemen zijn instructies vastgesteld om dit uit te voeren. De MIVD heeft aangegeven dat een groot deel van de Wiv 2002 gegevens die op de eigen systemen zijn opgeslagen, inmiddels op relevantie is beoordeeld. Er is een verlenging van een half jaar ingesteld voor het op relevantie beoordelen van de resterende Wiv 2002 data.

Voorts wordt gewerkt aan het realiseren van de relevantiebeoordeling door de MIVD van MIVD-data die op AIVD systemen staan opgeslagen. Dit is mede afhankelijk van een juiste technische koppeling tussen de systemen van de beide diensten. Ten aanzien van deze data volgt de MIVD het beleid van de AIVD en heeft de bewaartermijn van deze gegevens eveneens verlengd met een half jaar. De gegevens moeten vóór 1 november 2019 relevant beoordeeld of vernietigd zijn (zie hiervoor). De technische implementatie die nodig is voor de feitelijke vernietiging van gegevens, is nog niet gerealiseerd. Voor gegevens van de MIVD die op basis van de Wiv 2002 zijn verzameld met de toenmalige bevoegdheid van ongerichte interceptie geldt, net als bij de AIVD, dat deze vóór 1 mei 2021 relevant beoordeeld of vernietigd moeten zijn.

Het risico voor het zo spoedig mogelijk op relevantie beoordelen van gegevens wordt ook voor de MIVD **bijgesteld van gemiddeld naar beperkt**. Ook voor de MIVD geldt dat het komende half jaar zal moeten uitwijzen of deze beoordeling gehandhaafd kan worden.

3.3 Op welke wijze vindt relevantiebeoordeling plaats?

Eerder vastgestelde risico's

De AIVD heeft een systematiek van datareductie ontwikkeld die in technische zin goed wordt ondersteund. Relevantiebeoordeling kan met geautomatiseerde ondersteuning en/of handmatig plaatsvinden. De relevantiebeoordeling met geautomatiseerde ondersteuning was echter nog onvoldoende ingekaderd. De AIVD had onvoldoende helder vastgelegd in welke gevallen relevantiebeoordeling met geautomatiseerde ondersteuning geoorloofd is en hoe deze methode van relevantiebeoordeling zich verhoudt tot handmatige relevantiebeoordeling. Of de relevantie van gegevens herleidbaar is, werd bovendien niet intern gecontroleerd. Effectief toezicht hierop was dus nog niet mogelijk. De CTIVD beoordeelde het risico als gemiddeld.

De MIVD miste een goede ICT infrastructuur als basis voor een gedegen datareductie systematiek. Relevantiebeoordeling werd beperkt technisch ondersteund. *Data lineage* (oorsprong en verloop van data) was onvolledig en interne controle op de relevantiebeoordeling was niet realiseerbaar. Hierdoor was de relevantiebeoordeling in veel gevallen onvoldoende herleidbaar en effectief toezicht niet aan de orde. De CTIVD beoordeelde het risico als hoog.

Voortgang AIVD

De verplichte datareductie heeft concrete nadere invulling gekregen in beleid en werkinstructies van de AIVD. 1 mei 2019 is een belangrijke peildatum voor de dienst, omdat vanaf die datum de termijn van een jaar voor het beoordelen van de relevantie van gegevens verloopt die vanaf 1 mei 2018 zijn verzameld. Een verlenging van een half jaar is onder omstandigheden mogelijk. Per 1 mei 2019 diende het systeem van datareductie dus volledig werkend te zijn. Dit lijkt ook het geval. De CTIVD zal de komende periode een (technische) steekproef verrichten teneinde dit in de praktijk te toetsen.

In het beleid van de AIVD is opgenomen dat van relevantiebeoordeling met geautomatiseerde ondersteuning alleen gebruik mag worden gemaakt bij bepaalde bijzondere bevoegdheden, waaronder een gerichte tap of hack. In zo'n geval kan bij de aanvraag van een bijzondere bevoegdheid vooraf worden aangegeven dat de opbrengst van de inzet behorend bij een bepaald 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, zonder dat hieraan een inhoudelijke beoordeling vooraf gaat. Dit brengt immers het risico met zich mee dat niet relevante gegevens toch bewaard worden. Er kan wel sprake zijn van uitzonderingsgevallen, die alsdan goed gemotiveerd en vastgelegd moeten worden. Er vindt momenteel nader overleg plaats met de AIVD onder welke voorwaarden relevantiebeoordeling met geautomatiseerde ondersteuning kan plaatsvinden met voldoende waarborgen voor de rechtsbescherming van de burger daarbij. Het met geautomatiseerde ondersteuning vooraf als relevant aanmerken van gegevens is in de meeste gevallen op dit moment technisch nog niet mogelijk.

Interne controle op de herleidbaarheid van de relevantiebeoordeling is nog niet aan de orde. Dit hangt samen met enerzijds het vastleggen van een aanvullende motivering waarom gegevens relevant zijn beoordeeld (zie hiervoor) en anderzijds met de nadere inrichting en uitwerking van de zorgplicht. Effectief extern toezicht is nu nog niet mogelijk.

Het risico wordt voor de AIVD **gehandhaafd op gemiddeld**.

Voortgang MIVD

Bij de MIVD vindt relevantiebeoordeling per verwerkingssysteem handmatig plaats. Hiervoor zijn werkinstructies opgesteld. Relevantiebeoordeling met geautomatiseerde ondersteuning is niet aan de orde. Dit is alleen voor de selectiebevoegdheid gefaciliteerd en wordt besproken in hoofdstuk 4 onder verantwoorde databeperking in het kader van onderzoeksopdrachtgerichte interceptie. Het op relevantie beoordelen van gegevens door medewerkers in het inlichtingenproces wordt beperkt technisch gefaciliteerd. De MIVD heeft in enkele verwerkingssystemen wel verbeteringen kunnen realiseren.

De MIVD is medio april begonnen met een ICT-pilot gericht op het ontwikkelen van een moderne data architectuur. Dit zal naar verwachting ook mogelijkheden bieden voor het waarborgen van *data lineage* (oorsprong en verloop van data) en interne controle op de relevantiebeoordeling. Het betreft een meerjarig traject waarvan de einddatum nog niet is vastgesteld. In verband hiermee is de MIVD bezig met verschillende ICT-projecten die (moeten) voorzien in tussentijdse oplossingen. Zo wordt onder meer gewerkt aan het realiseren van relevantiebeoordeling door de MIVD van MIVD-data die op AIVD systemen staat opgeslagen.

Het risico wordt voor de MIVD **gehandhaafd op hoog**.

3.4 Hoe wordt gegarandeerd dat gegevens onomkeerbaar worden vernietigd wanneer dat door de wet wordt vereist?

Eerder vastgestelde risico's

Voor de tijdige vernietiging van gegevens is het, gegeven de omvang daarvan, absoluut noodzakelijk dat sprake is van een ondersteunende ICT infrastructuur die hier in kan voorzien. Bij de AIVD lijkt dit het geval en zou de inrichting van de systemen moeten voorzien in een tijdige vernietiging van gegevens. De mogelijkheid gegevens niet-relevant te verklaren was echter in veel gebruikte applicaties nog niet aanwezig. Ook was geen sprake van interne controle. De vernietiging van gegevens was

daarom nog niet goed toetsbaar door de CTIVD. De ICT infrastructuur van de MIVD en onvolledige *data lineage* (oorsprong en verloop van data) maakten dat een rechtmatige vernietiging van gegevens nog onvoldoende geborgd was, intern niet controleerbaar was en extern effectief toezicht niet mogelijk was. De CTIVD beoordeelde het risico voor de AIVD als gemiddeld en voor de MIVD als hoog.

Voortgang AIVD

De AIVD heeft gewerkt aan het aanpassen van applicaties die worden gebruikt voor de verwerking van gegevens, zodat elke applicatie de mogelijkheid biedt gegevens als niet-relevant aan te merken, waarop die gegevens vervolgens geautomatiseerd vernietigd worden. Inmiddels is dit voor de meeste applicaties gerealiseerd. Waar dit technisch niet mogelijk is, zijn maatregelen getroffen.

Onmiddellijke vernietiging van gegevens is niet in alle gevallen mogelijk. Soms duurt het enige tijd voordat gegevens technisch gezien vernietigd kunnen worden. De gegevens worden dan eerst verwijderd, dat wil zeggen ontoegankelijk gemaakt voor medewerkers in het inlichtingenproces. Dit levert geen wezenlijk risico op dat de gegevens alsnog gebruikt zullen worden.

Er is door de AIVD een audit uitgevoerd op een onderdeel van de datareductie systematiek, waaronder de vernietiging van gegevens. Dit is een eerste stap in de interne controle. In een structurele interne controle op de vernietiging van gegevens is nog niet voorzien, hetgeen samenhangt met de nadere inrichting en uitwerking van de zorgplicht.

Het risico wordt voor de AIVD **bijgesteld van gemiddeld naar beperkt**.

Voortgang MIVD

De inrichting van systemen voorziet gedeeltelijk in de geautomatiseerde vernietiging van gegevens. Dit betekent dat de vernietiging van gegevens in veel gevallen handmatig in gang moet worden gezet wanneer de gegevens als niet relevant zijn aangemerkt of wanneer de bewaartermijn is verlopen. In interne controle hierop is niet voorzien waardoor effectief toezicht op de vernietiging van gegevens niet mogelijk is.

De MIVD is medio april begonnen met een ICT-pilot gericht op het ontwikkelen van een moderne data architectuur. De verwachting is dat dit ook mogelijkheden zal bieden voor het geautomatiseerd vernietigen van gegevens. Zoals eerder is opgemerkt betreft dit een meerjarig traject waarvan de einddatum nog niet is vastgesteld. In verband hiermee is de MIVD bezig met het realiseren van tussentijdse oplossingen voor het geautomatiseerd vernietigen van gegevens.

Het risico wordt voor de MIVD **gehandhaafd op hoog**.

4 Onderzoeksopdrachtgerichte interceptie ether

Essentie wettelijke regeling

Een belangrijk toetsingscriterium voor de verzameling en verdere verwerking van gegevens is dat van 'zo gericht mogelijk'. Dit criterium moet niet alleen worden gemotiveerd in de verzoeken om toestemming voor de inzet van bijzondere bevoegdheden in het stelsel van onderzoeksopdrachtgerichte interceptie, maar dient vervolgens ook zijn werking te krijgen bij de toepassing daarvan in de praktijk. Concreet houdt die toepassing in dat o.m. de filtering van te intercepteren gegevens, de toekenning van selectiecriteria en bijvoorbeeld het gebruik van een profiel bij metadata-analyse 'zo gericht mogelijk' moeten zijn.

Databeperking vindt in het interceptieproces getrapt plaats. Filtering bepaalt welke gegevens worden opgeslagen en welke niet. Na filtering geldt een doorlopende vernietigingsplicht t.a.v. de opgeslagen gegevens. Een ander onderdeel van databeperking is het op relevantie beoordelen van gegevens nadat deze zijn geselecteerd op basis van selectiecriteria, zoals telefoonnummers, IP adressen of trefwoorden. De geselecteerde gegevens moeten worden beoordeeld op relevantie voor enig lopend onderzoek. Geselecteerde gegevens die niet relevant zijn, moeten worden vernietigd. De laatste stap betreft de vernietiging van niet op relevantie beoordeelde geïntercepteerde gegevens bij het aflopen van de bewaartermijn. Voor onderzoeksopdrachtgerichte interceptie van de ether geldt een bewaartermijn van maximaal drie jaar.

De volgende wettelijke en beleidsmatige waarborgen zijn in het kader van onderzoeksopdrachtgerichte interceptie van belang:

4.1 Is het toestemmingsproces adequaat ingericht?

Eerder vastgestelde risico's

Zowel het algemeen beleid als formats voor het opstellen van verzoeken om toestemming boden de medewerkers van de diensten in het algemeen voldoende handvatten voor het indienen van verzoeken om toestemming voor de inzet van bijzondere bevoegdheden in het proces van onderzoeksopdrachtgerichte interceptie. In de door de TIB rechtmatig bevonden verzoeken om toestemming waren alle wettelijk vereiste elementen opgenomen. De CTIVD zag geen aanleiding te toetsen of de verzoeken op inhoud voldeden aan de vereisten van de wet, dat was en is in beginsel aan de TIB. De CTIVD zag vanuit de inrichting van dit proces geen risico's op onrechtmatig handelen door de beide diensten

Voortgang AIVD en MIVD

In oktober 2018 bracht de TIB een brief uit over haar werkzaamheden vanaf 1 mei 2018. In de brief kwam tot uiting dat de verzoeken om toestemming voor de inzet van bijzondere bevoegdheden door de AIVD op onderdelen verbetering behoefden. Ook werd aangegeven dat 5,5% van de verzoeken van de AIVD was afgewezen tegenover 4,1% van de verzoeken van de MIVD. De AIVD heeft mede naar aanleiding hiervan een verbetertraject in gang gezet. Zo is er aandacht geweest voor het (aanvullend) opleiden van medewerkers van de dienst die belast zijn met het opstellen van verzoeken om toestemming. Ook is er een separaat team ingesteld, bestaande uit medewerkers met juridische, operationele en technische kennis, dat elk verzoek om toestemming controleert op volledigheid en inhoudelijke motivering. In haar jaarverslag over 2018 rapporteerde de TIB dat de kwaliteit van de verzoeken om toestemming van de AIVD is toegenomen. Voor de MIVD was er geen aanleiding een soortgelijk traject te starten.

De CTIVD ziet in de inrichting van dit proces voor de AIVD en de MIVD **geen risico** op onrechtmatig handelen.

4.2 Wordt toepassing gegeven aan het criterium ‘zo gericht mogelijk’?

Eerder vastgestelde risico’s

Aan het criterium ‘zo gericht mogelijk’ werd geen herkenbare invulling gegeven in het beleid en de werkprocessen van de beide diensten. Het beleid, de werkinstructies en de feitelijke werkprocessen van de beide diensten maakten niet duidelijk hoe ‘zo gericht mogelijk’ in de praktijk uitwerking kreeg. De toepassing van het criterium ten aanzien van de verschillende stadia van het interceptieproces leek vanaf 1 mei 2018 dus vrijwel achterwege te zijn gebleven, terwijl het juist daar een richtinggevende werking kan en moet hebben. De CTIVD beoordeelde het risico op onrechtmatige verzameling en verwerking van gegevens door de beide diensten als hoog.

Voortgang AIVD en MIVD

De AIVD heeft een juridisch kader (februari 2019) en beleid (maart 2019) opgesteld. De inhoud van deze stukken is grotendeels ook overgenomen in beleid van de MIVD (april 2019). Het beleid is vervolgens nog op onderdelen aangepast (mei 2019). In het beleid wordt uitgewerkt wat het criterium ‘zo gericht mogelijk’ inhoudt in het kader van onderzoeksopdrachtgerichte interceptie. Zo gericht mogelijk wil volgens het beleid van de beide diensten zeggen dat zij een redelijke inspanning moeten leveren bevoegdheden zo gericht mogelijk uit te oefenen en daarover verantwoording moeten afleggen. Dit is mede afhankelijk van 1) de bevoegdheid die wordt ingezet, 2) de aard van de gegevens en 3) de context van de gegevensverwerking. Met de toepassing van “zo gericht mogelijk” wordt beoogd de inbreuk op grondrechten van personen die geen onderwerp zijn van onderzoek te beperken.

De toepassing van ‘zo gericht mogelijk’ in het interceptiestelsel is in kwantitatieve zin vooral van betekenis bij de filtering van gegevens bij de interceptie zelf. Het beleid blijft op het punt van filtering vrij algemeen. Het stelt dát filters zo gericht mogelijk moeten zijn maar geeft niet aan op welke wijze dat vorm moet krijgen. Nadere precisering hoe een zo gerichte mogelijke filtering moet plaatsvinden, bijvoorbeeld in een werkinstructie, is van belang zodat sprake is van een duidelijke sturing op de praktijk van filtering. De CTIVD zal op deze praktijk nader ingaan in haar aankomende toezichtsrapport over de werking van filters, dat in de zomer van 2019 wordt gepubliceerd.

In het beleid van de AIVD en de MIVD is opgenomen dat ook de bevoegdheden van search, metadata-analyse en selectie ‘zo gericht mogelijk’ moeten worden ingezet en toegepast. Dit is in overeenstemming met de uitleg die de CTIVD geeft aan het criterium ‘zo gericht mogelijk’, dat zijn werking dient te hebben in alle fasen van het stelsel. Wat ‘zo gericht mogelijk’ concreet inhoudt is niet uitgewerkt voor metadata-analyse, maar wel voor de bevoegdheden van search en selectie. Zo volgt uit het beleid dat ruime selectiecriteria, zoals trefwoorden, goed moeten worden gemotiveerd en vermeld moet worden waarom de selectie niet gerichter kan. Op de toepassing hiervan in de praktijk zal de CTIVD nader ingaan in het haar aankomende toezichtsrapport over de toepassing van de selectiebevoegdheid, dat in de zomer van 2019 wordt gepubliceerd. De CTIVD acht het van belang dat het beleid ook duidelijkheid biedt wat een zo gericht mogelijke metadata-analyse inhoudt en dat in een werkinstructie wordt neergelegd hoe dit zijn uitwerking dient te krijgen bij de verschillende vormen van metadata-analyse.

Voor selectie zijn binnen de beide diensten naast beleid ook werkinstructies en/of procesbeschrijvingen opgesteld waarin nadere handvatten worden geboden voor een zo gericht mogelijke selectie.

Het risico wordt voor de AIVD en de MIVD **bijgesteld van hoog naar gemiddeld**.

4.3 Zijn voldoende waarborgen voor geautomatiseerde data-analyse aan de orde?

Eerder vastgestelde risico's

Het beleid en de werkprocessen van de beide diensten gaven onvoldoende houvast voor het rechtmatig toepassen van de geautomatiseerde analyse van metadata uit onderzoeksopdrachtgerichte interceptie ex. artikel 50 Wiv 2017 (metadata-analyse). De CTIVD stelde over de periode 1 mei tot 1 juli 2018 vast dat het proces met onvoldoende (procedurele) waarborgen was omkleed. Een systematiek van interne controle was bovendien niet ingericht. De CTIVD beoordeelde het risico op onrechtmatig handelen als hoog.

In hoofdstuk 5 wordt separaat ingegaan op dit onderdeel van het stelsel van onderzoeksopdracht-gerichte interceptie.

4.4 Is sprake van voldoende waarborgen voor de selectie van gegevens?

Eerder vastgestelde risico's

Door het selecteren van gegevens aan de hand van selectiecriteria wordt de inhoud van deze gegevens toegankelijk gemaakt voor medewerkers in het operationele proces. Het bepalen van de selectiecriteria gebeurt intern en dient gemotiveerd te worden. De diensten hadden uitgebreid beleid opgesteld ten aanzien van de selectie van inhoudelijke communicatie. De wettelijke vereisten waren daarin op een juiste wijze vastgelegd. Het beleid c.q. de werkinstructies van de beide diensten dienden nog aangevuld te worden t.a.v. de interne autorisatie van selectiecriteria en in beperkte mate t.a.v. het verwijderen van selectiecriteria. De CTIVD beoordeelde het risico voor beide diensten als beperkt.

Voortgang AIVD en MIVD

De interne autorisatie van selectiecriteria is bij beide diensten vastgelegd en verloopt procesmatig goed. De motivering voor de selectiecriteria is in het algemeen goed toetsbaar. Zodra de toestemming voor selectie vervalt, moeten de bijbehorende selectiecriteria worden verwijderd. Wanneer en op welke wijze dit plaatsvindt, wordt uitgelegd in werkinstructies bij de beide diensten. Het uitgangspunt is dat selectiecriteria moeten worden verwijderd als deze niet meer bruikbaar zijn voor het onderzoek of onjuiste gegevens opleveren. De AIVD heeft in het afgelopen half jaar problemen in het selectieproces ondervonden (zie hieronder). De systemen die de MIVD gebruikt voor de verwerking van gegevens uit onderzoeksopdrachtgerichte interceptie zijn overzichtelijk en functioneren naar behoren.

Selectieproblematiek AIVD

De AIVD heeft met de invoering van de Wiv 2017 hard gewerkt aan het aanpassen van applicaties die het etherinterceptiestelsel in technische zin ondersteunen. Verschillende applicaties bepalen in samenhang de wijze waarop de verwerving van gegevens van de ether, de opslag van gegevens na filtering en het selecteren van gegevens op basis van selectiecriteria plaatsvindt. De AIVD heeft de werking van de nieuw ontwikkelde of aangepaste applicaties wel getest, maar nog niet in onderlinge samenhang. In het najaar van 2018 heeft de AIVD geconstateerd dat er problemen waren met verschillende applicaties. Als gevolg hiervan heeft het selectieproces vanaf mei 2018 niet goed gefunctioneerd. Door de dienstleiding van de AIVD is meteen na het constateren van de problematiek een team ingesteld dat onderzoek heeft gedaan naar en sturing geeft aan het oplossen van de problemen en heeft hiervan melding gedaan aan de CTIVD. De AIVD heeft bij die onderdelen waar zich deze problemen manifesteerden de inzet van de interceptie- en selectiebevoegdheden stopgezet totdat de problemen zijn opgelost. In dat kader worden maatregelen getroffen teneinde een dergelijke situatie in de toekomst te voorkomen. De CTIVD houdt hier toezicht op.

Het risico wordt voor de AIVD en de MIVD **gehandhaafd op beperkt**.

4.5 Op welke wijze vindt relevantiebeoordeling plaats?

Eerder vastgestelde risico's

Databeperking vindt in het onderzoeksopdrachtgericht interceptieproces getrapt plaats, onder meer door de filtering en de selectie van gegevens. De relevantiebeoordeling van de inhoud van de verworven gegevens is een onderdeel hiervan. Dit proces is dus complexer dan datareductie van gegevens verzameld met de inzet van andere bijzondere bevoegdheden. Er werd door de AIVD en de MIVD nog onvoldoende invulling gegeven aan de verantwoorde beperking in het kader van het stelsel van onderzoeksopdrachtgerichte interceptie van ethercommunicatie. Er was geen specifiek beleid vastgesteld hiervoor. Het was onduidelijk op welke wijze de beoordeling van de relevantie van gegevens plaatsvindt, nadat de gegevens zijn geselecteerd aan de hand van selectiecriteria. Er was nog geen herkenbare en gestructureerde vorm van interne controle op de vernietiging van gegevens. De CTIVD beoordeelde het risico hier als hoog voor zowel de AIVD als de MIVD.

Voortgang AIVD en MIVD

De AIVD en de MIVD hebben in beleid opgenomen op welke wijze databeperking plaatsvindt in het kader van onderzoeksopdrachtgerichte interceptie. Dit valt grofweg uiteen in twee fasen: 1) databeperking door filtering bij de verwerving van gegevens en 2) het reduceren van gegevens tot datgene dat van belang is voor lopende onderzoeken.

Filtering is *kwantitatief* gezien het belangrijkste element bij de uitvoering van verantwoorde databeperking in het interceptiestelsel. Er is in beleid en procesbeschrijvingen aangegeven op welke wijze filtering grofweg plaatsvindt. De diensten hebben inspanningen geleverd de verschillende interceptiestromen in kaart te brengen, waarbij de verschillende keuzemomenten voor databeperking voldoende worden aangeven. Het beleid biedt echter geen concrete handvatten voor de (wijze van) de toepassing van filters. Het is van belang dat de diensten in werkinstructies specifieker ingaan op de overwegingen die een rol spelen bij de precieze instelling van filters, bij voorkeur per interceptiesysteem. Dergelijke werkinstructies zijn nog niet vastgesteld.

De relevantiebeoordeling van geselecteerde gegevens is *kwalitatief* gezien het belangrijkste element bij de uitvoering van verantwoorde databeperking in het interceptiestelsel. In beleid en werkinstructies is verwoord hoe dit in zijn werk gaat. Daarin is ook opgenomen dat gegevens die worden geselecteerd met 'gerichte' selectiecriteria, zoals een telefoonnummer, e-mailadres of IP-adres, zonder nadere beoordeling relevant kunnen worden verklaard. Deze gegevens kunnen geautomatiseerd als relevant worden gelabeld. Bij de inzet van 'minder gerichte' selectiecriteria, zoals een trefwoord, kan volgens het beleid de opbrengst niet op voorhand als relevant worden aangemerkt. Deze gegevens moeten eerst inhoudelijk beoordeeld worden. De CTIVD ziet geen wettelijke ruimte voor het categorisch op voorhand als relevant aanmerken van gegevens die zijn geselecteerd met een 'gericht' selectiecriterium. Het draagt het risico in zich dat niet relevante gegevens toch worden bewaard. Er kan wel sprake zijn van uitzonderingsgevallen, die alsdan goed gemotiveerd en vastgelegd moeten worden. De AIVD en de MIVD hebben beide besloten geen categorische benadering van het op voorhand als relevant aanmerken van gegevens te (zullen) hanteren. Er vindt momenteel nader overleg plaats met de AIVD en de MIVD onder welke voorwaarden relevantiebeoordeling met geautomatiseerde ondersteuning kan plaatsvinden met voldoende waarborgen voor de rechtsbescherming van de burger daarbij. De CTIVD toetst in haar lopende onderzoek naar de inzet van de selectiebevoegdheid in welke mate gegevens zonder nadere inhoudelijke beoordeling als relevant zijn aangemerkt en beoordeelt dit op rechtmatigheid.

Een knelpunt is het vernietigen van data die aan de beide diensten toebehoort en door óf de AIVD óf de MIVD als niet relevant is beoordeeld. De wet vereist onmiddellijke vernietiging van deze gegevens. Dit is problematisch wanneer de gegevens nog niet beoordeeld zijn of wél als relevant zijn aangemerkt door de andere dienst. Hier is vooralsnog geen goede technische oplossing voor gerealiseerd. De CTIVD zal hier in de volgende voortgangsrapportage aandacht aan besteden.

In interne controle is momenteel nog niet voorzien. Dit hangt ook samen met de nadere inrichting van de zorgplicht bij de beide diensten. De AIVD heeft een project opgezet om de ICT-infrastructuur voor onderzoeksopdrachtgerichte interceptie naar behoren te laten werken en controleerbaar te maken. Interne controle is beoogd met onder meer de inrichting van verschillende dashboards waarmee zal worden gemonitord op *compliance*. De verouderde ICT-infrastructuur bij de MIVD maakt het inbouwen van geautomatiseerde controlemechanismen niet goed mogelijk. Effectief extern toezicht door de CTIVD is nog niet mogelijk.

Het risico wordt voor de AIVD en de MIVD **bijgesteld van hoog naar gemiddeld**.

4.6 Is functie- en taakscheiding gewaarborgd waar dit vereist is?

Eerder vastgestelde risico's

Functie- en taakscheiding wil zeggen dat slechts aan bepaalde medewerkers de bevoegdheid wordt toegekend inhoudelijk kennis te mogen nemen van bepaalde gegevens en specifieke taken worden toegewezen die niet voor anderen gelden. Deze functie- en taakscheiding was nader beschreven in beleid en zorgde voor een specifiek en kenbaar onderscheid tussen medewerkers (o.m. volgens het *need to know* principe). In de praktijk was de scheiding echter diffuser. Hoewel niet wettelijk vereist, kan functie- en taakscheiding bovendien een waarborg vormen ter versterking van een rechtmatige toepassing van metadata-analyse. Dit was echter in beperkte mate ingericht. Verder was nog geen sprake van een intern controle mechanisme dat specifiek ziet op functie- en taakscheiding. De CTIVD constateerde een gemiddeld risico voor de AIVD en de MIVD.

Voortgang AIVD en MIVD

De AIVD en MIVD hebben de interne aanwijzing van functionarissen die kennis mogen nemen van inhoud van communicatie in het kader van onderzoeksopdrachtgerichte interceptie aangepast. Dit heeft geleid tot een verbetering in functie- en taakscheiding. Met de technische uitwerking met betrekking tot het bijhouden van de autorisaties is begonnen maar dit moet nog verder tot wasdom komen bij de beide diensten. De functie- en taakscheiding ziet wettelijk gezien op inhoud van gegevens. Het is daarom van belang dat dit begrip goed wordt afgebakend in relatie tot metadata en geïmplementeerd wordt in de technische systemen waar de AIVD en de MIVD gebruik van maken. Er is een definitie van inhoud en metadata in het beleid van de beide diensten opgenomen. De diensten hebben dit nader uitgewerkt, zodat het vervolgens in de praktijk technisch zal kunnen worden toegepast. Ook zal worden voorzien in een procedure voor heroverweging van wat als inhoud en als metadata wordt aangemerkt. Er is een start gemaakt met de interne controle op functie- en taakscheiding. In functie- en taakscheiding voor metadata is niet voorzien.

Het risico wordt voor de beide diensten **bijgesteld van gemiddeld naar beperkt.**

5 Metadata-analyse ex artikel 50 Wiv 2017

Essentie wettelijke regeling

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 de wet 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 (metadata-analyse). Deze toestemming wordt vervolgens op rechtmatigheid getoetst door de TIB. Pas dan mag de bevoegdheid worden toegepast. Op de uitvoering van de metadata-analyse wordt toezicht gehouden door de CTIVD.

Dit onderdeel van de wet lijkt vrij eenvoudig, maar is in de uitvoering in de praktijk complex. De TIB en de CTIVD hebben al in de zomer van 2018 besloten het onderwerp verder uit te diepen in hun rechtseenheid overleg, teneinde meer duidelijkheid te scheppen over het toetsingskader dat zij beiden toepassen bij de beoordeling van de verzoeken om toestemming respectievelijk de uitvoering daarvan. Dit dient niet alleen de rechtszekerheid van de burger, het geeft ook de beide diensten de benodigde houvast. Op 23 november 2018 is een rechtseenheidbrief over dit onderwerp verzonden aan de Eerste en Tweede Kamer en gepubliceerd op de websites van de TIB en de CTIVD.[5] De betrokken ministers hebben hierop gereageerd per brief van 19 maart 2019.[6]

Eerder vastgestelde risico's

De CTIVD constateerde in de eerste voortgangsrapportage dat het beleid en de werkprocessen van de beide diensten onvoldoende houvast boden voor het rechtmatig toepassen van de geautomatiseerde analyse van metadata uit onderzoeksopdrachtgerichte interceptie. De CTIVD stelde over de periode 1 mei tot 1 juli 2018 vast dat het proces met onvoldoende (procedurele) waarborgen was omkleed. Zij beoordeelde het risico op onrechtmatig handelen voor de AIVD en de MIVD als hoog.

Ook merkte de CTIVD in haar eerste voortgangsrapportage op dat er nader overleg had plaatsgevonden met de departementen van BZK en van Defensie en met de AIVD en de MIVD. Naar aanleiding hiervan was weliswaar een positieve ontwikkeling merkbaar bij de diensten, maar bleef er een fundamenteel verschil van opvatting bestaan over wat wettelijk wordt verstaan onder de geautomatiseerde analyse van metadata, tussen de TIB en de CTIVD enerzijds en de beide diensten en departementen anderzijds.

Steekproef

De CTIVD heeft in oktober en november 2018 een steekproef uitgevoerd naar de toepassing van metadata-analyse op het data platform van de AIVD met behulp van een drietal applicaties, waar ook de MIVD gebruik van maakt. De steekproef beoogde twee vragen te beantwoorden:

1. Vindt de door de diensten verrichte metadata-analyse rechtmatig plaats, d.w.z. binnen een verleende toestemming?
2. Kan de CTIVD effectief toezien op de uitvoering van de metadata-analyse?

Metadata-analyse bestaat uit geautomatiseerde gegevensverwerkingen. Om na te kunnen gaan welke gegevensverwerking plaats heeft gevonden is geautomatiseerde vastlegging van elke handeling noodzakelijk. Zonder die vastlegging (logbestanden) is het niet goed mogelijk een beeld te krijgen van de metadata-analyse die is verricht. Met deze steekproef is naar een beperkt deel van de systemen en applicaties van de beide diensten gekeken. De CTIVD heeft logbestanden opgevraagd van drie applicaties met betrekking tot een periode van een week. Dit betrof een zoek-applicatie, een netwerkanalyse-applicatie en een applicatie om query's (SQL) uit te kunnen voeren. De aangeleverde

5 *Kamerstukken II* 2018/19, 29924, nr. 174.
6 *Kamerstukken II* 2018/19, 29924, nr. 179.

logbestanden komen voort uit gestructureerde en geautomatiseerde vastlegging ten behoeve van interne controle op informatieveiligheid.

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. De logbestanden zelf misten essentiële gegevens. Benodigde aanvullende informatie om de logbestanden nader te kunnen duiden waren niet integraal beschikbaar. Evenmin kon geautomatiseerd worden herleid wie er precies toegang had tot de data en applicaties, vanuit welke functie of taak in het inlichtingenproces. Zonder deze gegevens is het niet mogelijk vast te stellen in het kader van welk onderzoek een metadata-analyse is uitgevoerd en of hiervoor toestemming is verkregen. De CTIVD constateerde dat zij onvoldoende kon herleiden of metadata-analyse rechtmatig heeft plaatsgevonden. Ook de AIVD zelf was hier niet toe in staat, aangezien het bestaande interne controle mechanisme uitsluitend zag op informatiebeveiliging en niet was ingericht vanuit het oogpunt van naleving van de wet *(compliance)*. Er was geen sprake van adequate interne controle en effectief extern toezicht was niet mogelijk.

Voortgang AIVD en MIVD

De AIVD en de MIVD hebben een intern verbod ingesteld op het verrichten van metadata-analyse, totdat intern voldoende helder was wat de reikwijdte is van artikel 50 Wiv 2017.[7] Aan metadata-analyse is aandacht besteed in het overkoepelende beleid van de beide diensten voor onderzoeksopdrachtgerichte interceptie (maart 2019). Specifiek beleid en werkinstructies zijn nog niet vastgesteld.

Naar aanleiding van de steekproef hebben gesprekken plaatsgevonden met de AIVD en de MIVD over de inrichting van een intern controle mechanisme, wat ook de CTIVD in staat moet stellen effectief toezicht uit te oefenen. Zo wordt onder meer gesproken over aanpassing van loggegevens en het gebruik van dashboards of geautomatiseerde management rapportages van de data-analyse die heeft plaatsgevonden. Een werkend mechanisme is voorzien voor 1 augustus 2019. De CTIVD zal in het najaar van 2019 opnieuw een steekproef verrichten en de werking hiervan toetsen.

In het verlengde van de rechtseenheidbrief van de TIB en de CTIVD is veelvuldig met de beide diensten en met de betrokken departementen gesproken over de toepassing van het wettelijk kader. Het wettelijk kader is helder: elke vorm van metadata-analyse die is gericht op het identificeren van personen en organisaties valt onder de regeling van artikel 50 Wiv 2017. Over grofweg twee onderwerpen bestaat er nog geen volledige overeenstemming. Ten aanzien van deze onderwerpen zal in de praktijk een goede balans moeten worden gevonden tussen de operationele werkbaarheid en de rechtsbescherming van de burger bij de toepassing van metadata-analyse.

Het eerste betreft de mate van abstractie of 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 nu zaak dat de juiste mate van abstractie of detail wordt bereikt, waarmee zowel een gedegen rechtmatigheidstoets kan plaatsvinden als voldoende operationele ruimte wordt geboden. De praktijk moet dit uitwijzen.

7 Dit verbod gold niet voor metadata-analyse ten behoeve van *force protection*, waarvoor door de minister van Defensie toestemming was verleend die door de TIB als rechtmatig is beoordeeld.

Het tweede onderwerp betreft de mate van inmenging in de persoonlijke levenssfeer die bij metadata-analyse aan de orde is. Niet elke metadata-analyse kent dezelfde mate van inmenging. Het gevoelen bestaat dan dat wanneer sprake is van een beperkte inbreuk, de regeling van artikel 50 Wiv 2017 administratief disproportioneel zwaar is. Om die reden is door met name de beide diensten gezocht naar het kunnen maken van een onderscheid. Ook de beide ministers hebben in hun reactie op de rechtseenheidbrief hieraan gerefereerd. Wat dit echter gecompliceerd maakt is dat een onderscheid niet goed te maken is in eenvoudige of complexe vormen van metadata-analyse. Ook een eenvoudige vorm zoals het combineren van twee gegevens kan, zeker in de combinatie van meerdere toepassingen daarvan, een aanzienlijk inmenging in de persoonlijke levenssfeer opleveren. Bovendien hoeft het niet zo te zijn dat een complexe vorm van metadata-analyse zoals het toepassen van een profiel, altijd een grote inbreuk oplevert. Zo is ook van belang welke data wordt betrokken bij de analyse en wat de beoogde toepassing is van de uitkomst. Het is met andere woorden context afhankelijk. De beide ministers hebben aangegeven dat met het oog op de wetsevaluatie te starten voor mei 2020, ervaring moet worden opgedaan met de toepassing van waarborgen voor metadata-analyse. Op basis daarvan zal deze discussie verder vorm kunnen krijgen.

Het risico wordt **bijgesteld van hoog naar gemiddeld**.

Postbus 85556
2508 CG Den Haag

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