Toezichtrapport

Filteren uit een ongerichte stroom gegevens: werking en waarde van het filterkader

CTIVD nr. 85

Vastgesteld op 15 juli 2026

Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten

Commissie van Toezicht
op de Inlichtingen- en
Veiligheidsdiensten

CTIVD nr. 85

TOEZICHTRAPPORT

Filteren uit een ongerichte stroom gegevens: werking en waarde van het filterkader

Inhoudsopgave

Publiekssamenvatting **2**

1. Hoofdboodschap **5**

2. OOG-interceptie: een korte introductie **6**

3. Onderzoeksaanpak **8**
3.1 Aanleiding onderzoek 8
3.2 Wat is er onderzocht? 8
3.3 Aanpak 9
3.4 Leeswijzer 9

4. De reductie van gegevens door het filterkader **10**
4.1 Het filterkader, leads en selectoren kunnen de onderschepte gegevens alle drie direct filteren 10
4.2 Het filterkader draagt bij aan datareductie, maar is voor de diensten ook van belang om onderzoek te kunnen doen naar ongekende dreigingen 12
4.3 Filtering vanwege beperkte (opslag) capaciteit leidt tot extra datareductie 13

5. Controle over de verwerking van gegevens **14**
5.1 Begrippen en definities worden inconsistent gebruikt 14
5.2 Het is niet altijd duidelijk of er enkel metadata wordt opgeslagen op basis van het filterkader 15
5.3 Het compliance raamwerk en de bestaande processen verkleinen het risico op onrechtmatigheden 15

Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten

Filteren uit een ongerichte stroom gegevens: werking en waarde van het filterkader

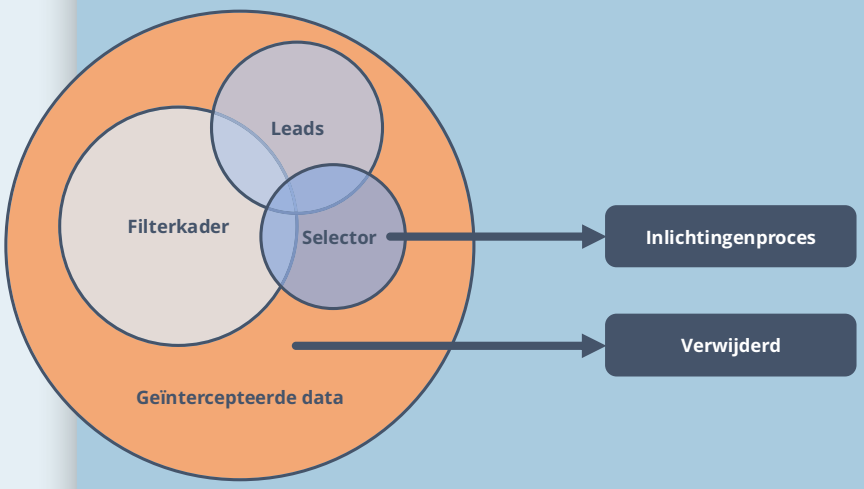
Samenvatting van de bevindingen uit het CTIVD-onderzoek (rapport 85)

Bevindingen over de reductie van gegevens door het filterkader

1. Het filterkader, *leads* en selectoren filteren alle drie direct de onderschepte gegevens (zie het kader hiernaast).
2. Het filterkader is van belang om onderzoek te kunnen doen naar ongekende dreigingen en moet daarom breed worden ingestoken. Dit heeft tot gevolg dat er ook meer gegevens door het gebruik van het filterkader worden opgeslagen die mogelijk na beoordeling niet-relevant blijken te zijn.
3. Filtering vanwege beperkte (opslag)capaciteit leidt tot extra datareductie.

Toelichting: het filterkader, *leads* en selectoren kunnen de onderschepte gegevens alle drie direct filteren

Deze drie typen filters zijn afzonderlijke methodes om gegevens uit de geïntercepteerde gegevensstromen op te slaan. Het proces van datareductie hoeft dus **geen trechter** te zijn, maar kan gelijktijdig plaatsvinden. *Leads* hoeven niet binnen het filterkader te vallen en selectoren niet binnen *leads*. Gegevens die geselecteerd worden op basis van selectoren worden opgeslagen ten behoeve van het inlichtingenproces, onafhankelijk van het filterkader (zie onderstaand schema).



Schematische weergave filtering. Let op: de omvang van de cirkels weerspiegelt niet de daadwerkelijke aantallen.

De interceptie van een bepaalde gegevensstroom kan worden goedgekeurd met een filterkader als waarborg. Selectoren van een ander onderzoek kunnen worden gebruikt om gegevens te selecteren uit dezelfde gegevensstroom. Dit betekent dat onderschepte gegevens ook kunnen worden geraadpleegd voor andere onderzoeken dan waarvoor de gegevens in eerste instantie zijn onderschept. De wet biedt hier ruimte voor, maar het is de vraag of de wetgever deze werkwijze en de gevolgen ervan heeft voorzien tijdens het wetgevingsproces.

Controle op de verwerking van gegevens

Er zijn procedures ingevoerd die bijdragen aan de zorgvuldige verwerking van gegevens. Daarnaast signaleert de CTIVD ook een aantal risico's:

1. De diensten gebruiken begrippen en definities inconsistent.
2. In sommige gevallen mag alleen metadata worden opgeslagen als gegevens bewaard worden door het filterkader. Het is niet duidelijk of dit in de praktijk zo is.
3. Er ontbreekt een aantal controles die bijdragen aan de goede werking van het filterkader.

Vervolg

1. De CTIVD doet aanbevelingen om de controle over de verwerking van gegevens te vergroten.
2. De CTIVD monitort de uitvoering hiervan in het doorlopend toezicht.
3. De CTIVD gaat onderzoek doen naar de werking van *leads* en selectoren.

Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten

Filteren uit een ongerichte stroom gegevens: werking en waarde van het filterkader

Achtergrond OOG-interceptie en het toezicht van de CTIVD

OOG-interceptie

De AIVD en de MIVD (hierna: de diensten) onderscheppen voor hun onderzoeken grote hoeveelheden communicatiegegevens. Dit wordt onderzoeksopdrachtgerichte (OOG) interceptie genoemd. Dit gaat bijvoorbeeld om gegevens die worden verstuurd via internetkabels of satellieten. Het is hierbij onvermijdelijk dat ook gegevens worden onderschept van personen of organisaties waar de diensten geen onderzoek naar doen. Daarmee maken de diensten inbreuk op de privacy van personen. Daarom gelden strikte voorwaarden voor het inzetten van deze bevoegdheid en voor de verwerking van onderschepte gegevens.

Datareductie

Niet alle onderschepte gegevens zijn interessant om te bewaren. Na het onderscheppen van gegevens worden deze gegevens teruggebracht tot gegevens die mogelijk relevant zijn voor lopende onderzoeken. De diensten moeten de gegevens die niet relevant zijn verwijderen. Dit proces heet datareductie. Hierdoor wordt de inbreuk op privacy van personen verkleind.

Filterkader

Het filterkader is één onderdeel van het proces van datareductie. Door middel van breed omschreven criteria (filters) worden gegevens doorgelaten die samenhangen met één of meerdere onderzoeken van de diensten. Een filter kan bijvoorbeeld zijn: *"één van de betrokken apparaten in de onderschepte communicatie is te relateren aan een onderzoek naar land X"*. De gegevens die het filterkader doorlaat, worden alleen onderzocht door speciaal hiervoor aangewezen medewerkers. Dit gebeurt bijvoorbeeld om zogenoemde nieuwe *leads* en/of selectoren te vinden.

Toezicht

De Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (CTIVD) houdt toezicht op de rechtmatige uitvoering van bevoegdheden door de diensten. De CTIVD bewaakt de balans tussen het waarborgen van de nationale veiligheid en de inbreuk op fundamentele rechten. In de eerste helft van 2026 heeft de CTIVD specifiek onderzoek gedaan naar het filterkader.
Het doel van het onderzoek was om diepgaande kennis te verkrijgen over het filterkader. Ook heeft de CTIVD onderzocht of het filterkader bijdraagt aan de rechtmatige inzet van de bevoegdheid tot ongerichte onderschepping van gegevens. De CTIVD heeft onder andere gekeken naar:

- de technische werking van het filterkader; en
- de wijze waarop de diensten controle houden op het proces van datareductie.

Later dit jaar zal de CTIVD ook onderzoek doen naar *leads* en selectoren, de andere onderdelen van het proces van datareductie.

De OOG-keten

De AIVD en MIVD bepalen in vier stappen of onderschepte gegevens relevant zijn voor hun onderzoeken. De handelingen binnen de OOG-keten hebben allemaal hun eigen waarborgen. Voor iedere handeling moet steeds toestemming aan de minister worden gevraagd.

Verkennen

- De diensten onderscheppen een korte periode een brede stroom aan gegevens.
- Op basis hiervan bepalen zij welke communicatiestroom relevante gegevens bevat om te onderscheppen.
- De gegevens die in deze fase worden onderschept, worden niet gebruikt in onderzoeken en maar korte tijd bewaard.

↓

Onderscheppen

- De diensten onderscheppen doorlopend een gegevensstroom die relevante informatie bevat voor de onderzoeken van de diensten.

↓

Datareductie

- De onderschepte gegevens worden teruggebracht naar gegevens die mogelijk relevant zijn. Niet-relevante gegevens moeten worden verwijderd.
- De diensten passen drie typen filters toe die samenhangen met hun onderzoeken:
  - Het filterkader: breed omschreven criteria.
  - *Leads*: zoekvragen die horen bij gekende en ongekende dreigingen, bijv. werkwijze van een organisatie in onderzoek is bij de diensten of een kenmerk waarvan nog niet is vastgesteld dat het toebehoort aan een target.
  - Selectoren: bekende kenmerken van personen die in onderzoek zijn bij de diensten.
- Gegevens die worden doorgelaten op grond van het filterkader en *leads*, komen niet rechtstreeks in het inlichtingenproces terecht. Deze gegevens worden alleen onderzocht door speciaal hiervoor aangewezen medewerkers om eventuele nieuwe *leads* of selectoren te vinden.

↓

Inlichtingenproces

- Inlichtingenteams gebruiken de gegevens voor hun onderzoeken naar dreigingen tegen de nationale veiligheid.
- Dit zijn alleen gegevens die worden bewaard op grond van selectoren.

Commissie van Toezicht
op de Inlichtingen- en
Veiligheidsdiensten

CTIVD nr. 85

TOEZICHTRAPPORT

Filteren uit een ongerichte stroom gegevens:
werking en waarde van het filterkader

1. Hoofdboodschap

De AIVD en de MIVD (‘**de diensten**’) zetten de bevoegdheid om ongericht gegevens te onderscheppen steeds vaker in. Deze bevoegdheid heet onderzoeksopdrachtgerichte interceptie (‘**OOG-interceptie**’). De afdeling toezicht van de CTIVD (hierna: CTIVD) onderzoekt de inzet van deze bevoegdheid door middel van drie themaonderzoeken.

Het is bij OOG-interceptie onvermijdelijk dat ook gegevens worden onderschept van personen of organisaties die niet in onderzoek zijn bij de diensten. Daarmee maken de diensten inbreuk op privacy van personen. Om de inbreuk te beperken is het belangrijk dat niet-relevante gegevens zo snel mogelijk worden verwijderd (‘**datareductie**’). Het gebruik van het filterkader is één stap in dit proces. Dit rapport gaat over de resultaten van het onderzoek naar het filterkader en over hoe het filterkader bijdraagt aan de rechtmatige inzet van OOG-interceptie.

Uit het onderzoek blijkt dat het filterkader bijdraagt aan datareductie. Een substantieel deel van de onderschepte gegevens wordt namelijk niet opgeslagen door het gebruik van het filterkader. Het filterkader is echter niet de enige stap in het proces van datareductie. Als gegevens niet worden opgeslagen op basis van het filterkader, dan blijkt uit het onderzoek dat deze gegevens alsnog kunnen worden opgeslagen op basis van (het gebruik van) twee andere methoden om te filteren. Dit betekent dat onderschepte gegevens ook kunnen worden geraadpleegd voor andere onderzoeken dan waarvoor de gegevens in eerste instantie zijn onderschept. De wet biedt hier ruimte voor, maar het is de vraag of de wetgever deze werkwijze heeft voorzien tijdens het wetgevingsproces. Daarnaast blijkt dat de diensten het filterkader soms ruim opstellen, zodat zij onderzoek kunnen doen naar dreigingen die nog niet bekend zijn (‘**ongekende dreigingen**’). Dit heeft tot gevolg dat er ook meer gegevens door het gebruik van het filterkader worden opgeslagen die mogelijk na beoordeling niet-relevant blijken te zijn. Ten slotte blijkt uit het onderzoek dat de diensten momenteel niet alle geïntercepteerde gegevens opslaan vanwege beperkte capaciteit voor opslag en transport.

De CTIVD signaleert een aantal risico’s voor de zorgvuldige verwerking van gegevens in de werkwijze van de diensten. Zo gebruiken de diensten begrippen en definities inconsistent, bijvoorbeeld met betrekking tot het verschil tussen metadata en inhoud. Ook ontbreken een aantal controles die kunnen bijdragen aan een goede werking van het filterkader. Tegelijkertijd constateert de CTIVD dat de diensten ook procedures hebben die de risico’s op onrechtmatigheden verkleinen.

Voordat de CTIVD ingaat op het onderzoek is in hoofdstuk 2 van dit rapport een korte uitleg over OOG-interceptie opgenomen.

2. OOG-interceptie: een korte introductie

Communicatiestromen zoals internetverkeer, lopen deels door de lucht en deels door kabels. De AIVD en MIVD mogen deze communicatiestromen ongericht onderscheppen. Het gaat hierbij om de gegevens van veel mensen en organisaties. Het is onvermijdelijk dat ook gegevens worden onderschept van personen of organisaties die niet in onderzoek zijn bij de diensten. Daarom gelden er strikte voorwaarden voor het inzetten van deze bevoegdheid en voor de verwerking van onderschepte gegevens.

De diensten gebruiken de onderschepte gegevens voor hun onderzoeken. In vier stappen wordt bepaald of de onderschepte communicatie van belang is voor deze onderzoeken. Deze stappen vormen de zogenaamde OOG-keten:

1. **Verkennen**
   Voordat de diensten langdurig communicatie gaan onderscheppen voor hun inlichtingen-onderzoeken, kunnen zij eerst onderzoeken of er op een datakabel of satellietverbinding relevante gegevens zitten. Hiervoor onderscheppen de diensten voor een korte periode een brede stroom aan gegevens die zij vervolgens onderzoeken. Dit heet *snapshotten* als dit gebeurt op grond van de Wet op de inlichtingen- en veiligheidsdiensten 2017 ('**Wiv 2017**') en verkennen als dit gebeurt op grond van de Tijdelijke Wet onderzoeken AIVD en MIVD naar landen met een offensief cyber-programma, bulkdatasets en overige specifieke voorzieningen ('**Tijdelijke wet**'). Met de kennis die de diensten opdoen met verkennen, kunnen ze vervolgens motiveren waarom en hoe ze een bepaalde communicatiestroom willen onderscheppen voor hun inlichtingenonderzoeken naar dreigingen tegen de nationale veiligheid. De informatie die de diensten verzamelen met verkennen, mogen zij niet in een inlichtingenonderzoek gebruiken. Ook bewaren de diensten deze informatie maar voor een beperkte tijd.

2. **Onderscheppen**
   Als de diensten weten waar voor hen relevante gegevens te vinden zijn, dan vragen zij jaarlijks toestemming aan de minister om deze gegevensstroom doorlopend te onderscheppen. In een verzoek om toestemming beschrijven de diensten welke gegevensstromen ze willen onderscheppen en wat ze vervolgens met die gegevens willen doen. In dat verzoek beschrijven de diensten ook hoe zij aan datareductie zullen doen.

3. **Datareductie**
   De diensten brengen de gegevens die zij onderscheppen zoveel mogelijk terug tot alleen de gegevens die (in potentie) relevant zijn voor lopende onderzoeken van de diensten. Niet-relevante gegevens moeten worden verwijderd. Dit wordt datareductie of filteren genoemd. Datareductie gebeurt door middel van drie verschillende typen filters: het filterkader, *leads* en selectoren. Alle drie de filters worden direct op de onderschepte gegevensstroom toegepast. De begrippen worden in het kader verder uitgelegd.

Filterkader (minst specifiek): door middel van (een combinatie van) breed omschreven criteria worden onderschepte gegevens doorgelaten die samenhangen met onderzoeken van de diensten. Een filter kan bijvoorbeeld zijn: *"één van de betrokken apparaten in de onderschepte communicatie is te relateren aan een onderzoek naar land X"*. Door het filterkader breed in te steken, kunnen de diensten ook onderzoek doen naar ongekende dreigingen. De gegevens die het filterkader doorlaat, worden alleen onderzocht door speciaal hiervoor aangewezen medewerkers. Dit gebeurt bijvoorbeeld om eventuele nieuwe *leads* en/of selectoren te vinden. Deze gegevens komen niet terecht in het inlichtingenonderzoek[1]. Dit wordt functiescheiding genoemd.

Als er in deze rapportage wordt gesproken over gegevens die door het filterkader komen, dan betekent dit dat die gegevens matchen met minimaal één van de filters in het filterkader.

***Leads* (gemiddeld specifiek):** zijn filters die de diensten gebruiken om gegevens die horen bij gekende en ongekende dreigingen op te slaan. *Leads* worden bijvoorbeeld gebaseerd op informatie die de diensten hebben over de werkwijze van een mogelijk doelwit. Een *lead* kan bijvoorbeeld zijn: *"een malwaresoort die vaak wordt gebruikt door een target"*. Een *lead* kan ook een kenmerk zijn waarvan nog niet is vastgesteld dat het toebehoort aan een target.

Selectoren (meest specifiek): dit zijn al bekende kenmerken van personen die in onderzoek zijn bij de diensten. Een voorbeeld van een selector is "het telefoonnummer van target". Alleen gegevens die horen bij een selector worden doorgestuurd naar medewerkers in het inlichtingen-proces.

1 Hierop bestaat één uitzondering: indien er toestemming is voor geautomatiseerde data-analyse zoals bedoeld in artikel 50 lid 1 onder b Wiv 2017, kunnen gegevens die door het gebruik van het filterkader worden opgeslagen wel in het inlichtingenproces komen. Dit valt buiten de scope van dit onderzoek.

4. Inlichtingenproces

De inlichtingenteams gebruiken gegevens verkregen met OOG-interceptie voor inlichtingen-onderzoeken naar dreigingen tegen de nationale veiligheid. Dit kan alleen wanneer deze gegevens worden doorgelaten op grond van selectoren. De inlichtingenteams kunnen deze gegevens gebruiken om informatie te achterhalen over personen, organisaties of onderwerpen waar onderzoek naar wordt gedaan. Als de diensten deze informatie hebben, dan kunnen zij die informatie ook gebruiken om in te schatten hoe concreet een dreiging is of andere overheidsinstanties informeren. Gegevens die worden doorgelaten op grond van het filterkader en *leads*, komen niet rechtstreeks in het inlichtingenproces terecht. Deze gegevens worden alleen onderzocht door speciaal hiervoor aangewezen medewerkers om eventuele nieuwe *leads*, respectievelijk selectoren te vinden.

De handelingen binnen de OOG-keten hebben allemaal hun eigen waarborgen. Voor iedere handeling moet steeds toestemming aan de minister worden gevraagd. Ook toetst de onafhankelijke Toetsingscommissie Inzet Bevoegdheden ('**TIB**') deze toestemming. In ieder toestemmingsverzoek moeten de diensten beargumenteren waarom de inzet van de bevoegdheid noodzakelijk, gericht en proportioneel is. Ook moeten ze afwegen of het resultaat niet met een lichter middel behaald kan worden ('**subsidiariteit**'). De manier waarop wordt omgegaan met datareductie en de functiescheiding spelen bij deze afwegingen een belangrijke rol.

3. Onderzoeksaanpak

Eind 2025 heeft de CTIVD aangekondigd onderzoek te doen naar de inzet van OOG-interceptie door middel van drie themaonderzoeken en doorlopend toezicht. Dit rapport bevat de uitkomsten van het eerste themaonderzoek. De CTIVD doet onderzoek naar OOG-interceptie omdat de inzet van deze bevoegdheid is toegenomen na de inwerkingtreding van de Tijdelijke wet.

OOG-interceptie: de bevoegdheid van de diensten om ongericht communicatie te onderscheppen die via de lucht of de kabel wordt verzonden. Er is hierbij sprake van onderschepping van grote hoeveelheden gegevens.

Datareductie: de diensten brengen de onderschepte gegevens terug tot die gegevens die (in potentie) relevant zijn voor lopende onderzoeken van de diensten. Niet-relevante gegevens moeten worden verwijderd.

3.1 Aanleiding onderzoek

Zoals hiervoor omschreven, worden bij OOG-interceptie ook altijd gegevens onderschept van personen en organisaties die geen onderwerp van onderzoek van de diensten zijn en dit ook niet zullen worden. Het toepassen van filters is een belangrijke stap in het proces van datareductie. Een deel van de datareductie vindt plaats door middel van de toepassing van filters in het filterkader. Deze filtering is van groot belang voor het beperken van de inbreuk. Het weegt daarom zwaar in de toetsing van de gerichtheid en proportionaliteit van de inzet van de bevoegdheid.

3.2 Wat is er onderzocht?

Het doel van het onderzoek is om diepgaande kennis te verkrijgen over het filterkader. Ook onderzoekt de CTIVD of de werkwijze van het filterkader bijdraagt aan de rechtmatige inzet van OOG-interceptie. Het onderzoek ziet allereerst op de technische werking van het filterkader. De CTIVD onderzoekt bijvoorbeeld de werking van concrete filters. Daarnaast ziet het onderzoek op de wijze waarop de diensten controle houden op het proces van datareductie.

In dit onderzoek kijkt de CTIVD specifiek naar de mate waarin het filterkader bijdraagt aan datareductie. In de loop van 2026 verwacht de CTIVD verder onderzoek te doen naar de functiescheiding en naar het filteren op basis van *leads* en selectoren. Hierover zullen afzonderlijke rapporten worden geschreven. Dit rapport bevat wel een bevinding over de verhouding tussen het filterkader, *leads* en selectoren. Deze verhouding is van belang voor de vraag in hoeverre het filterkader bijdraagt aan de reductie van gegevens.

Dit rapport ziet op de AIVD en de MIVD. De inzet van OOG-interceptie wordt uitgevoerd binnen de Joint Sigint Cyber Unit (**'JSCU'**) van de AIVD en de MIVD. De bevindingen van dit onderzoek zijn daarom van toepassing op beide diensten.

3.3 Aanpak

De CTIVD voerde de afgelopen jaren doorlopend gesprekken over OOG-interceptie met de diensten. Het filterkader was onderdeel van deze gesprekken. Dit themaonderzoek is gestart met een kort vooronderzoek in de systemen van de diensten. Vervolgens heeft de CTIVD gesprekken gevoerd met medewerkers en aanvullende vragen gesteld.

De CTIVD beoordeelt de rechtmatigheid van het werk van de diensten. Het toetsingskader hierbij is de Wiv 2017 en de Tijdelijke wet. De CTIVD maakt in haar oordelen onderscheid tussen (on)rechtmatig en (on)zorgvuldig handelen. Waar nodig doet de CTIVD aanbevelingen.

Onrechtmatig: de diensten handelen in strijd met de wet als bijvoorbeeld als niet wordt voldaan aan de wettelijke vereisten van noodzakelijkheid, proportionaliteit en subsidiariteit. De diensten handelen ook onrechtmatig als een wettelijke grondslag voor handelen ontbreekt.

Onzorgvuldig: er is een tekortkoming in beleid, werkwijze of processen die (toekomstige) onrechtmatigheden in de hand kan werken.

3.4 Leeswijzer

Ieder hoofdstuk start met een korte conclusie. De bevindingen en begrippen in deze conclusie legt de CTIVD uit in het hoofdstuk zelf. De bevindingen zijn donkerblauw cursief weergegeven. De hoofdstukken bevatten ook kleurenkaders. De betekenis van de kaders is als volgt:

- Blauwe kaders bevatten uitleg over gebruikte terminologie of wetgeving.
- Paarse kaders bevatten aanbevelingen.
- Oranje kaders bevatten een voorbeeld.

4. De reductie van gegevens door het filterkader

Dit hoofdstuk gaat in op de vraag of en op welke wijze het filterkader leidt tot reductie van gegevens. Op basis van het onderzoek komt de CTIVD tot een aantal conclusies:

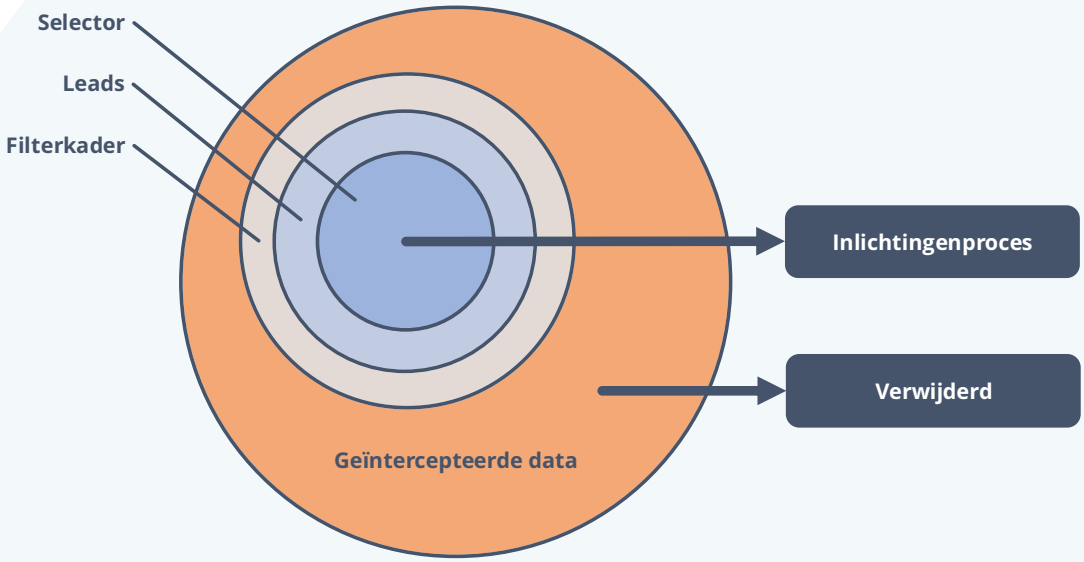
1. Het filterkader, *leads* en selectoren kunnen de onderschepte gegevens alle drie direct filteren. De wet biedt hier ruimte voor, maar het is de vraag of de wetgever dit heeft voorzien.
2. Het filterkader draagt bij aan datareductie, maar is voor de diensten ook van belang om onderzoek te kunnen doen naar ongekende dreigingen.
3. Filtering vanwege beperkte capaciteit leidt tot extra datareductie.

Deze conclusies worden hieronder afzonderlijk toegelicht.

4.1 Het filterkader, leads en selectoren kunnen de onderschepte gegevens alle drie direct filteren

De toelichting op de Wiv 2017 en de Tijdelijke wet beschrijft de OOG-keten als een proces van datareductie dat bestaat uit verschillende stappen of fasen. De wetsgeschiedenis beschrijft dat alleen de gegevens worden opgeslagen als zij vallen binnen het filterkader, *leads* of selectoren. De rest van de onderschepte gegevens worden verwijderd.

De wetgever hanteert in de beschrijving van de verschillende stappen of fasen woorden die wijzen op een bepaalde volgordelijkheid, zoals *"aansluitend"*, *"fase 1 en 2"*, *"hierna"* en *"vervolgens"*. Hierdoor lijkt het er op alsof de filterstappen elkaar telkens in dezelfde volgorde opvolgen. Het beeld ontstaat dat *leads* binnen het filterkader en selectoren binnen *leads* moeten vallen. Hierbij zorgt de functiescheiding ervoor dat alleen aangewezen medewerkers in de gegevens die opgeslagen worden door het filterkader, kunnen zoeken naar nieuwe *leads* en/of selectoren. Alleen gegevens die worden opgeslagen op basis van selectoren worden uiteindelijk gebruikt in het inlichtingenproces. Deze werkwijze wordt geïllustreerd in Figuur 1. Daarin geeft de oranje cirkel de onderschepte gegevens weer en de blauwe cirkels het filterkader, de *leads* en de selectoren.

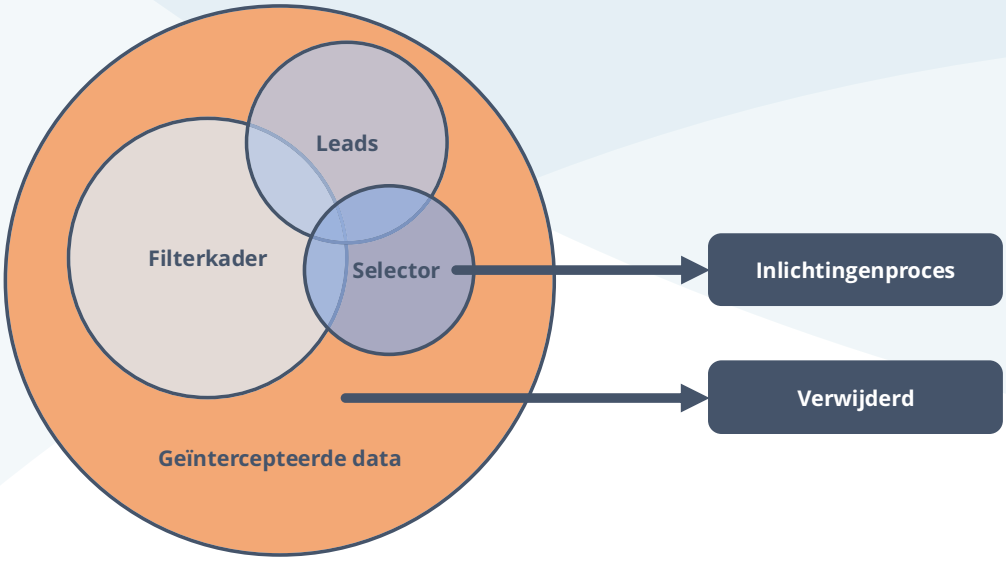


Figuur 1, schematische weergave filtering (perceptie op basis van wetsgeschiedenis). Let op: de omvang van de cirkels weerspiegelt niet de daadwerkelijke aantallen.

Voorbeeld bij Figuur 1: de diensten onderscheppen ongericht een brede stroom gegevens. Zij hebben toestemming om dit te doen in het kader van een onderzoek naar land X. Het filterkader richt zich dan op gegevens die te relateren zijn aan een onderzoek naar dat land. Tijdens een onderzoek van gegevens die door het filterkader en/of de *leads* komen, ontdekken de diensten een nieuw kenmerk van een persoon die in onderzoek is bij de diensten. Het inlichtingenteam dat onderzoek doet naar land X voegt dit kenmerk vervolgens toe als selector. Het inlichtingenteam ontvangt dan de gegevens die daaraan gekoppeld zijn. De volgorde van Figuur 1 wordt dan gevolgd. De betreffende selector valt dan immers binnen een (eerder opgevoerde) *lead* en de *lead* valt binnen het (eerder opgevoerde) filterkader.

Dit beeld klopt maar gedeeltelijk. Het proces van datareductie is in de praktijk niet altijd een opeenvolgend proces, maar een proces dat ook naast elkaar en gelijktijdig kan plaatsvinden. De diensten passen bepaalde *leads* en selectoren in de praktijk ook rechtstreeks toe op de stroom met onderschepte gegevens. Hierdoor slaan de diensten ook gegevens op als deze horen bij een door een inlichtingenteam opgegeven selector, zonder dat deze gegevens worden opgeslagen op grond van het filterkader of *leads*. Dit wordt weergegeven in Figuur 2.

Figuur 2 laat zien dat een groot deel van de geïntercepteerde gegevens niet wordt opgeslagen (het oranje deel). Het filterkader, *leads* en selectoren (de blauwe cirkels) slaan onafhankelijk van elkaar gegevens op. Dit neemt niet weg dat het in de praktijk zo kan zijn dat er overlap is tussen de verschillende onderdelen. Bijvoorbeeld als de situatie van het voorbeeld bij Figuur 1 zich voordoet. In alle gevallen geldt dat alleen gegevens die worden opgeslagen op basis van selectoren beschikbaar zijn voor verdere verwerking in het inlichtingenonderzoek. Gegevens die worden doorgelaten op grond van het filterkader en *leads*, komen niet rechtstreeks in het inlichtingenproces terecht. Deze gegevens worden alleen onderzocht door speciaal hiervoor aangewezen medewerkers om eventuele nieuwe *leads* of selectoren te vinden.



Figuur 2, schematische weergave filtering (realiteit). Let op: de omvang van de cirkels weerspiegelt niet de daadwerkelijke aantallen.

De situatie die Figuur 2 weergeeft betekent dat de diensten de onderschepte stroom aan gegevens voor verschillende onderzoeken kunnen gebruiken. Hierbij geldt de waarborg dat zij voor ieder onderzoek toestemming vragen aan de minister, die door de TIB op rechtmatigheid wordt beoordeeld. Het kan zo zijn dat deze verschillende onderzoeken geen verband met elkaar houden. Of dit leidt tot resultaten, is afhankelijk van de breedte van de onderschepte gegevensstroom en de aard van de gegevens. Dit varieert per gegevensstroom.

Voorbeeld bij Figuur 2: de diensten onderscheppen ongericht een brede stroom gegevens. Zij hebben toestemming om dit te doen in het kader van een onderzoek naar land X. Het filterkader richt zich dan op gegevens die zijn te relateren dat onderzoek. Dit betekent dat alleen gegevens die met een onderzoek naar land X te maken hebben door het filterkader komen.

Daarnaast doet de dienst onderzoek naar dreiging A. Deze dreiging is niet gerelateerd aan land X. Het inlichtingenteam dat hiermee bezig is, heeft toestemming om gegevens te selecteren op basis van bijvoorbeeld een telefoonnummer van een persoon. De gegevens die worden doorgelaten door deze selector zijn beschikbaar voor het team dat onderzoek doet naar dreiging A.

De werkwijze van het naast elkaar toepassen van filterkader, *leads* en selectoren is niet onrechtmatig. De wet biedt deze ruimte. Gegevens die met OOG-interceptie worden onderschept kunnen ook worden gebruikt voor andere onderzoeken dan waarvoor de interceptietoestemming is verleend. De CTIVD vindt het belangrijk dat deze werkwijze bekend is. Het is namelijk de vraag of de wetgever de huidige werkwijze heeft voorzien, aangezien dit niet aan bod komt in de wetsgeschiedenis. Deze werkwijze heeft echter wel gevolgen voor het hele systeem van datareductie. Niet alleen het filterkader is een belangrijke waarborg, maar ook de breedte van de gegevensstroom en de reikwijdte van de *leads* en selectoren die op een datastroom worden toegepast zijn van belang. Bredere *leads* en selectoren kunnen leiden tot opslag van meer gegevens en daarmee tot een grotere inbreuk op rechten van personen. Om deze reden zal de CTIVD op een later moment apart onderzoek doen naar *leads* en selectoren.

4.2 Het filterkader draagt bij aan datareductie, maar is voor de diensten ook van belang om onderzoek te kunnen doen naar ongekende dreigingen

Ongekende dreiging: In tegenstelling tot gekende dreigingen, staan ongekende dreigingen nog niet op de radar van de diensten. Het gaat hierbij onder meer om methodes, individuen en organisaties waarvan op dit moment nog niet bekend is dat zij mogelijke dreigingen zijn voor de nationale veiligheid. Bijvoorbeeld nog niet onderkende terroristische cellen, nieuwe cyberdreigingen en capaciteiten of intenties ten aanzien van het gebruik of de ontwikkeling van massavernietigingswapens. Vanwege de ongerichtheid van OOG-interceptie, is dit een bruikbaar middel voor de diensten om deze ongekende dreigingen bloot te leggen. Wel geldt hierbij ook de voorwaarde dat de gegevens die worden opgeslagen, te relateren moeten zijn aan concrete onderzoeken van de diensten.

De hoeveelheid gegevens die wordt gefilterd door het filterkader is afhankelijk van de gegevensstroom, de interceptietechniek en van het type onderzoek. In het algemeen wordt een substantieel percentage van de totale hoeveelheid geïntercepteerde gegevens niet opgeslagen. Hiermee concludeert de CTIVD dat het filterkader dus bijdraagt aan datareductie.

Daarnaast geldt in de meeste gevallen dat alleen toestemming is verkregen voor het opslaan van metadata (en dus geen inhoud) als gegevens door het filterkader komen. De CTIVD is van oordeel dat deze keuze in belangrijke mate kan bijdragen aan datareductie.

Tegelijkertijd maakt het filterkader het ook mogelijk voor de diensten om breder gegevens te onderscheppen. Dit is nodig om ongekende dreigingen te onderzoeken. Door het analyseren van metadata kunnen verbanden en patronen aan het licht komen die er op het eerste gezicht niet lijken te zijn. Hiervoor zijn filters nodig die breder zijn dan *leads* en selectoren. De breedte van het filterkader is in de praktijk afhankelijk van het onderzoek waarvoor wordt geïntercepteerd. Voor onderzoeken naar cyberdreigingen is een breder filterkader sneller proportioneel dan wanneer onderzoek wordt gedaan naar specifieke personen of organisaties. Dit betekent dat er op dit moment meer gegevens worden opgeslagen ten behoeve van onderzoek naar cyberdreigingen.

4.3 Filtering vanwege beperkte (opslag) capaciteit leidt tot extra datareductie

De diensten moeten ook filteren vanwege de beperkte beschikbaarheid van ruimte om gegevens op te slaan of te transporteren. Daarom doen de diensten aan zogenaamde capacitaire filtering. Dit gebeurt momenteel grotendeels willekeurig. De gegevens die vanwege capacitaire filtering niet worden opgeslagen, kunnen ook niet worden bevraagd op grond van *leads* en selectoren. In die zin kan capacitaire filtering als een extra reductieslag worden gezien, nog voordat de hiervoor beschreven filtering plaatsvindt. Wel merkt de CTIVD hierbij op dat deze wijze van datareductie afhankelijk is van de mate waarin de diensten in staat zijn opslagcapaciteit beschikbaar te maken voor OOG-interceptie. Dit betekent dat deze waarborg in de toekomst eventueel komt te vervallen wanneer de diensten meer capaciteit hebben.

5. Controle over de verwerking van gegevens

Dit hoofdstuk gaat in op de vraag of en op welke wijze de diensten controle hebben op de werking en impact van het filterkader. De CTIVD komt tot de volgende conclusies met betrekking tot de zorgvuldige verwerking van gegevens:

1. Begrippen en definities worden inconsistent gebruikt.
2. Het is niet altijd duidelijk of er enkel metadata wordt opgeslagen op basis van het filterkader.
3. Het compliance raamwerk en de bestaande processen verkleinen het risico op onrechtmatigheden.
4. Er zijn geen standaard controles wanneer er veranderingen in datastromen plaatsvinden.

Deze conclusies worden hieronder afzonderlijk toegelicht.

Zorgplicht: de diensten hebben de plicht om ervoor te zorgen dat gegevens zorgvuldig worden verwerkt. Ze moeten zorgen voor een goede beveiliging en voorkomen dat de gegevens worden verwerkt terwijl hiervoor geen toestemming is. De diensten moeten hiervoor de nodige technische, personele en organisatorische maatregelen treffen, zodat ze voortdurend controle hebben over de wijze waarop gegevens worden verwerkt.

Dit is van belang voor de diensten, maar ook voor de samenleving. Dit beperkt immers de inbreuk van de inzet van het middel en vergroot de waarde voor de onderzoeken van de diensten. Als filterkaders niet goed functioneren, dan ontstaat het risico dat de diensten bepaalde gegevens onterecht bewaren of dat de diensten onvoldoende onderzoek kunnen doen naar (ongekende) dreigingen.

De CTIVD heeft in het licht van het uitgangspunt van voortdurende controle over gegevensverwerking en de hiervoor genoemde verantwoordelijkheid onderzoek gedaan naar de werkwijzen en processen met betrekking tot het filterkader.

5.1 Begrippen en definities worden inconsistent gebruikt

De wet en de toelichting daarop geven definities aan verschillende concepten binnen de OOG-keten. Deze juridische definities zijn vaak complex en de technische implementatie daarvan kan beperkingen met zich meebrengen. Uit de gevoerde gesprekken en de bestudeerde beleidsdocumenten blijkt dat de diensten definities inconsistent gebruiken. Een voorbeeld hiervan is het gebruik van de term *snapshotten* voor twee verschillende processen. Deze term gebruiken de diensten voor het verkennen van gegevensstromen voorafgaand aan het langdurig onderscheppen van gegevens. Ook gebruiken zij het voor het verkennen van gegevensstromen ten behoeve van technische optimalisatie wanneer gegevensstromen worden onderschept voor het gebruik in het inlichtingenonderzoek. Ook kunnen definities contextafhankelijk zijn. Een voorbeeld hiervan wordt in de tweede bevinding van dit hoofdstuk beschreven.

Inconsistent gebruik van definities en/of verschil in taalgebruik tussen juridische en technische medewerkers vergroot de kans op onduidelijkheid en misverstanden. Deze onduidelijkheid kan zowel intern optreden tussen dienstmedewerkers als extern tussen diensten en toezichthouders. Naar het oordeel van de CTIVD is dit onzorgvuldig, aangezien dit het risico op onrechtmatigheden vergroot.

Aanbeveling: implementeer een werkwijze waarin definities consistent worden gebruikt en niet contextafhankelijk zijn.

5.2 Het is niet altijd duidelijk of er enkel metadata wordt opgeslagen op basis van het filterkader

Metadata: de gegevens over communicatie. De metadata van een telefoongesprek zijn bijvoorbeeld de betrokken telefoonnummers, de start- en eindtijd van een gesprek en de gegevens van betrokken telefoonmasten.

Onderschepte gegevens bevatten zowel metadata als inhoud van communicatie. De diensten leggen deze begrippen niet consistent uit. De diensten gebruiken bijvoorbeeld samenvoegingen zoals *"technische metadata"* of *"juridische inhoud"*, of andersom. Op basis hiervan is onduidelijk wanneer welke onderdelen van communicatie als metadata worden beschouwd en wanneer als inhoud. Zo kan het onderwerp van een bericht onder bepaalde omstandigheden inhoud zijn, maar technisch worden behandeld als metadata. Dit kan leiden tot onduidelijkheden.

Bovendien worden de termen verschillend gebruikt in de toestemmingsverzoeken om gegevens te onderscheppen. Uit het onderzoek is gebleken dat in de meeste gevallen toestemming is gegeven om alleen metadata op te slaan als gegevens worden bewaard op basis van het filterkader. In die gevallen moeten de diensten ervoor zorgen dat sommige delen van de metadata niet worden opgeslagen. Bijvoorbeeld als de metadata ook het onderwerp van een bericht bevat. Ook zijn er toestemmingsverzoeken goedgekeurd waarin geen begrenzing is opgenomen om alleen metadata te bewaren. In die gevallen mag dus ook inhoud worden opgeslagen. Dit verschil in toestemmingsverzoeken brengt het risico op onrechtmatigheden met zich mee, omdat daardoor voor ieder onderzoek afzonderlijke afwegingen moeten worden gemaakt.

Er worden verschillende definities en werkwijzen gehanteerd, waardoor onduidelijk is of er in de praktijk inderdaad alleen metadata wordt opgeslagen. De CTIVD meent dat het goed zou zijn dat de afweging om gegevens als metadata of als inhoud te kwalificeren, worden beschreven in de toestemmingsverzoeken. Op die manier kan dit worden meegenomen in de toetsing van de gerichtheid en proportionaliteit.

Aanbeveling: wees consistent in het gebruik van definities en zorg voor een consistente werkwijze voor ieder toestemmingsverzoek.

5.3 Het compliance raamwerk en de bestaande processen verkleinen het risico op onrechtmatigheden

De diensten hebben verschillende hulpmiddelen om ervoor te zorgen dat de toepassing van het filterkader in de praktijk past binnen de grenzen van de verkregen toestemming. Een voorbeeld hiervan is het gebruik van een 'compliance kader'. Hierin zijn de belangrijkste passages uit het toestemmingsverzoek opgenomen. Uit het compliance kader kunnen uitvoerende, meestal technische

medewerkers, onder andere overzichtelijk opmaken binnen welke juridische kaders zij uitvoering moeten geven aan het filterkader. Dit voorkomt dat hiervoor telkens het hele toestemmingsverzoek moet worden onderzocht. Wanneer er incidenten plaatsvinden, wordt dit compliance kader ook gebruikt als toetsingskader.

Ook is sprake van vier-ogen-controles op zowel de technische implementatie van het filterkader als de juridische reikwijdte van de toegepaste filters. De CTIVD vindt beide constateringen positief. Deze hulpmiddelen verkleinen het risico op onrechtmatigheden.

Wel is gebleken dat de vier-ogen-controles in de praktijk soms onvolledig zijn. Dit is bijvoorbeeld het geval waar de vier-ogen-controle alleen ziet op de vraag of de technische implementatie (dat wil zeggen de geschreven code) klopt. Hierbij wordt niet meegenomen of het toegepaste filter ook binnen de omschrijving in het toestemmingsverzoek en dus binnen de juridische kaders past. De CTIVD concludeert dat de werkwijze in de praktijk maar beperkt bijdraagt aan het verkleinen van het risico op onzorgvuldigheden en/of onrechtmatigheden.

Aanbeveling: maak duidelijk wat een vier-ogen-controle inhoudt.

4. Er zijn geen standaard controles wanneer er veranderingen in datastromen plaatsvinden

De diensten kunnen verschillende soorten gegevensstromen onderscheppen. Iedere gegevensstroom is verschillend, bijvoorbeeld omdat de aard van de gegevens anders is. In de praktijk verklaren de diensten delen van het filterkader van toepassing op verschillende gegevensstromen of op nieuwe gegevensstromen. De mate waarin een bestaand filterkader kan bijdragen aan reductie van nieuwe gegevensstromen is afhankelijk van de aard van de gegevens die worden onderschept. Gedurende enige periode was er geen standaard controle ingericht voor de situatie waarin de aard van de gegevensstroom wijzigt.

Deze werkwijze heeft geleid tot een incident waarbij meer gegevens werden opgeslagen dan waarvoor toestemming was verleend. De diensten hebben dit intern adequaat onderzocht. Uitkomst van het interne onderzoek was dat het filter niet voldoende specifiek was. Vervolgens hebben de diensten hun beleid aangepast met betrekking tot het testen van filters. Als een nieuwe gegevensstroom wordt toegevoegd, dan moeten de filters eerst worden getest voordat deze in gebruik worden genomen.

Deze wijziging houdt echter geen rekening met een situatie waarin de aard van een gegevensstroom wijzigt die al doorlopend wordt onderschept. In die situatie kan het gebeuren dat gegevens die niet relevant zijn voor de diensten worden opgeslagen op basis van de filters in het filterkader, omdat de aard van de gegevens inmiddels is gewijzigd. Naar het oordeel van de CTIVD is dit onzorgvuldig, aangezien dit het risico op onrechtmatigheden vergroot.

Aanbeveling: zorg voor een werkwijze die rekening houdt met wijzigingen in gegevensstromen.

Postbus 85556, 2508 CG Den Haag

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