Bijlage I: Toetsingskader

bij het toezichtsrapport over de inzet van kabelinterceptie door de AIVD en de MIVD

De snapshotfase

CTIVD nr. 75

Vastgesteld op 26 januari 2022

Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten

Commissie van Toezicht
op de Inlichtingen- en
Veiligheidsdiensten

CTIVD nr. 75

BIJLAGE I: TOETSINGSKADER

bij het toezichtsrapport over de inzet van kabelinterceptie door de AIVD en de MIVD

Inhoudsopgave

Commissie van Toezicht
op de Inlichtingen- en
Veiligheidsdiensten

CTIVD nr. 75

BIJLAGE I: TOETSINGSKADER

bij het toezichtsrapport over de inzet van kabelinterceptie door de AIVD en de MIVD

1. Inleiding

De Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (hierna: CTIVD) beantwoordt in dit toezichtsrapport de vraag of de Algemene Inlichtingen- en Veiligheidsdienst (hierna: AIVD) en de Militaire Inlichtingen- en Veiligheidsdienst (hierna: MIVD) in de periode van 1 mei 2018 tot en met 31 maart 2021 op rechtmatige wijze een zogenoemde accesslocatie hebben geoperationaliseerd en op rechtmatige wijze uitvoering hebben gegeven aan de bevoegdheid van kabelinterceptie in de snapshotfase. De diensten hebben in deze periode de kabel aftapbaar gemaakt en interceptie van die kabel toegepast. De kabelinterceptie vond plaats in de vorm van het snapshotten. Dat is het uitvoeren van kortstondige integrale interceptie van gegevensstromen. De opgeslagen gegevens worden vervolgens aan de hand van technische en inhoudelijke kenmerken onderzocht op relevantie voor één of meerdere onderzoeksopdrachten van de diensten. In de onderzoeksperiode zijn daarbij waarborgen toegepast om de inbreuk op fundamentele rechten van burgers te beperken.

De Wiv 2017 kent geen specifieke bevoegdheid voor het snapshotten. In de praktijk voeren de diensten het snapshotten uit op basis van artikel 48 (interceptie). Het onderzoek op de gegevens vindt plaats op grond van artikel 49 lid 1 (*search* gericht op interceptie).

Kabelinterceptie

Interceptie op de kabel houdt in dat de AIVD en de MIVD grote hoeveelheden kabelgebonden communicatie kunnen intercepteren zonder dat deze interceptie gericht is op een specifiek target, zoals een persoon of een organisatie. De interceptie dient wel te relateren zijn aan één of meerdere onderzoeksopdrachten van de diensten, die weer voortvloeien uit de Geïntegreerde Aanwijzing (hierna: GA). Bij deze inherent ongerichte vorm van interceptie onderscheppen de diensten (op grote schaal) gegevens van personen die geen onderwerp van hun onderzoek zijn en dat ook nooit zullen zijn. Grote gegevensverzamelingen die voor het (overgrote) merendeel bestaan uit gegevens van personen die geen onderwerp van onderzoek zijn, worden bulkdatasets genoemd. Daarom wordt deze vorm van interceptie aangeduid als bulkinterceptie. De CTIVD wil in dit rapport verwarring tussen de termen OOG-interceptie, bulkinterceptie of ongerichte interceptie op de kabel vermijden en spreekt in dit rapport daarom zoveel mogelijk van kabelinterceptie.

Toetsingskader

In dit toetsingskader wordt ingegaan op de juridische vereisten die van toepassing zijn op zowel het operationaliseren van de accesslocatie als op het uitvoeren van de interceptie. Zij vormen het

toetsingskader voor het diepteonderzoek naar de inzet van kabelinterceptie door de AIVD en de MIVD.[1] Het kader is gebaseerd op de Wiv 2017 en de beleidsregels, de parlementaire geschiedenis, eventueel relevante jurisprudentie, eerdere toezichtsrapporten en door de ministers van Binnenlandse Zaken en Koninkrijksrelaties (hierna: BZK) en van Defensie in dat verband overgenomen aanbevelingen.

Het toetsingskader is als volgt opgebouwd. Hoofdstuk 2 bespreekt de relevante algemene bepalingen uit de Wiv 2017 voor gegevensverzameling en gegevensverwerking. Hoofdstuk 3 gaat in op het juridisch kader dat geldt voor het operationaliseren van de accesslocatie. Hoofdstuk 4 bespreekt vervolgens de kaders voor het uitvoeren van de interceptie. Het toetsingskader sluit af met hoofdstuk 5 waarin een samenvatting wordt gegeven van de wettelijke vereisten.

Verwijzingen naar wetgeving

In dit toetsingskader verwijst de CTIVD veelvuldig naar artikelnummers uit wetgeving. Tenzij expliciet anders aangegeven, verwijst de CTIVD daarmee naar de Wiv 2017.

1 Dit toetsingskader ziet op de beginfase van het interceptieproces (artt. 48, 49 lid 1, 52 en 53 Wiv 2017). Zie voor een uitleg over de verschillende fasen hoofdstuk 4 van dit toetsingskader. Voor de wettelijke bepalingen ten aanzien van de volgende fasen van het interceptieproces wordt verwezen naar de toetsingskaders van twee rapporten van de CTIVD; rapport 63 over de toepassing van filters bij OOG-interceptie door de AIVD en de MIVD en rapport 64 over de inzet van de bijzondere bevoegdheid tot selectie bij OOG-interceptie door de AIVD en de MIVD. Deze rapporten zien op OOG-I in de ether.

2. Algemene bepalingen Wiv 2017

Voor de verwerking van gegevens voor de uitvoering van de taken van de diensten gelden de algemene vereisten van gegevensverwerking. De algemene bepalingen voor gegevensverwerking zijn vastgelegd in de artikelen 17 tot en met 24. 'Verwerken' is een breed begrip. Onder het verwerken van gegevens valt onder andere het verzamelen, vastleggen, ordenen, raadplegen en het verstrekken van gegevens.[2] Daarnaast gelden voor de inzet van algemene en bijzondere bevoegdheden algemene bepalingen die van toepassing zijn op de verzameling van gegevens (artikelen 25 tot en met 31). In dit hoofdstuk worden niet alle algemene bepalingen besproken die gelden voor het verzamelen van gegevens en het verwerken van de gegevens. Dit zou te omvangrijk zijn.

Door de CTIVD is geen onderzoek gedaan naar de motivering van de verzoeken tot toestemming, omdat deze reeds door de Toetsingscommissie Inzet Bevoegdheden (hierna: TIB) op rechtmatigheid zijn beoordeeld. Dat betekent dat de CTIVD niet opnieuw heeft getoetst op de algemene vereisten van noodzakelijkheid, proportionaliteit en subsidiariteit. Een uitzondering vormt het gerichtheidsvereiste. Dit heeft de CTIVD in haar toets betrokken, omdat de ministers van BZK en van Defensie haar expliciet hebben verzocht daarover te rapporteren.[3]

Doelbinding en noodzakelijkheid (artikel 18)

De verwerking van gegevens mag slechts plaatsvinden voor een bepaald doel en voor zover dat noodzakelijk is voor de uitvoering van de taakstelling van de diensten. Dit wordt in de Wiv 2017 doelbinding en het noodzakelijkheidsvereiste genoemd.[4] Het doel van de gegevensverwerking dient ook te worden vastgelegd in de motivering van een toestemmingsaanvraag voor de inzet van een bevoegdheid.[5] De diensten moeten daarbij de verwachting hebben dat door de verwerking van de gegevens dat doel ook kan worden bereikt en dienen dit te kunnen onderbouwen.[6] De diensten dienen in de toestemmingsaanvraag te motiveren waarom de inzet van de bijzondere bevoegdheid noodzakelijk is, waarbij zij de proportionaliteit en de subsidiariteit expliciet moeten afwegen.[7]

Zorgplicht (artikel 24)

De hoofden van de AIVD en de MIVD zijn verantwoordelijk voor de toepassing van technische, personele en organisatorische maatregelen voor een rechtmatige gegevensverwerking.[8] De bevordering van de kwaliteit van de gegevensverwerking voor een rechtmatige gegevensverwerking is een nieuw vereiste ten opzichte van de oude Wiv 2002. De zorgplicht vraagt nadrukkelijk meer van de AIVD en de MIVD dan slechts het invoeren van de verplichtingen die de wet hen oplegt bij onder meer de verzameling, analyse en het feitelijk gebruik van de gegevens door medewerkers van de diensten.[9]

De zorgplicht houdt onder meer 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*). Beleid, procesbeschrijvingen en werkinstructies, waarbij oog is voor het beleggen van rollen en verantwoordelijkheden, kunnen daaraan bijdragen.

2 Artikel 1 onder f Wiv 2017.
3 Brief aan de Voorzitter van de Eerste Kamer d.d. 6 april 2018, *Kamerstukken I* 2017/18, 34588, G.
4 Artikel 18 Wiv 2017.
5 Zie ook rapport nr. 38 (2014), p. 29.
6 Zie rapport nr. 56 (2018) over de multilaterale gegevensuitwisseling door de AIVD over (vermeende) jihadisten, bijlage II, p. 2.
7 *Kamerstukken II* 2016/17, 34588, nr. 3, p. 47.
8 Artikel 24 lid 2 onder a Wiv 2017.
9 Zie ook rapport nr. 59 (2018), p. 7.

Voortdurend *in control* zijn vereist ook dat de diensten een aantal instrumenten gebruiken dat hen (centraal) zicht geeft op de werking van processen en systemen van gegevensverwerking en hen daardoor in staat stelt tijdig risico's te signaleren en passende maatregelen te nemen. Dit is niet alleen van belang voor de eigen interne controle, maar ook voor het mogelijk maken van effectief toezicht door de CTIVD.

Proportionaliteit en subsidiariteit (artikel 26)

Proportionaliteit houdt in dat een afweging wordt gemaakt tussen het doel dat wordt nagestreefd en het nadeel voor de betrokkene. Met het nadeel voor de betrokkene wordt bedoeld de inbreuk op de fundamentele rechten van de betrokkene die daarmee gepaard gaat. De uitoefening van de bevoegdheid dient daarbij evenredig te zijn met het daarmee beoogde doel.

De subsidiariteitstoets houdt in dat de AIVD of de MIVD moet kiezen voor de bevoegdheid die het minst ingrijpend is voor de betrokkene.[10] De inzet van bijzondere bevoegdheden, zoals kabelinterceptie, worden doorgaans als ingrijpender voor de betrokkene beschouwd dan de inzet van algemene bevoegdheden.

Zo gericht mogelijk (art. 26)

Naar aanleiding van de implementatie van de aangenomen motie van (destijds) Tweede Kamerlid Recourt (*Kamerstukken II* 2016/17, 34588, nr. 66) moet de bevoegdheid tot kabelinterceptie 'zo gericht mogelijk' worden ingezet. Conform de toezegging van het kabinet in de brief van 6 april 2018 aan de beide Kamers is op 25 april 2018 een beleidsregel gepubliceerd waarin onder meer is opgenomen dat de toepassing van bijzondere bevoegdheden door de diensten zo gericht mogelijk dient plaats te vinden.[11] Met de wetswijziging van 15 juli 2021 is deze toezegging opgenomen in artikel 26. Het gerichtheidscriterium is van toepassing op het gehele interceptieproces. In het verzoek om toestemming als bedoeld in artikel 29 dient nadrukkelijk te worden aangegeven op welke wijze aan de eis van gerichte inzet van de desbetreffende bijzondere bevoegdheid invulling wordt gegeven. In de wetsgeschiedenis wordt echter niet aangegeven wat het vereiste van 'zo gericht mogelijk' precies inhoudt.

Voor de definitie van het gerichtheidsvereiste heeft de regering ervoor gekozen aan te sluiten bij het door de TIB gehanteerde criterium.[12] De regering geeft in de toelichting op het wijzigingsvoorstel Wiv 2017 een zo concreet mogelijke invulling aan het begrip 'zo gericht mogelijk':

"De diensten moeten zo goed als redelijkerwijs mogelijk is (en voor zover van toepassing) in het verzoek om toestemming de eis van gerichtheid invullen door de te vergaren gegevens af te bakenen: geografisch, naar tijdstip, naar soort data/type verkeer, naar object/target, naar gedraging of anderszins. Daarbij moet onder meer rekening worden gehouden met de inlichtingencontext waarin juist naar de tot dan toe ongekende dreiging moet worden gezocht, met de fase waarin het onderzoek zich bevindt, met de noodzaak tot falsificatie, met het tijdselement en de reële technische mogelijkheden."[13]

De regering wijst erop dat voorgaand criterium ruimte laat om het verzamelen onder omstandigheden breder en minder gericht te laten plaatsvinden. Zo kunnen beperkingen in de techniek ertoe leiden dat het niet mogelijk is om een bepaalde 'knip' aan te brengen in de dataset die wordt verzameld en om deze reden de gehele set wordt verzameld. Ook is de fase waarin het onderzoek zich bevindt bepalend. In de verkennende fase zal het in eerste instantie (veelal) onvermijdelijk zijn om bevoegdheden breder in

10 *Kamerstukken II* 2016/17, 34588, nr. 3, p. 202.
11 Artikel 5 Beleidsregels Wiv 2017.
12 "[I]n hoeverre is bij verwerving sprake van het tot een minimum beperken van niet strikt voor het onderzoek noodzakelijke gegevens, gelet op de technische en operationele omstandigheden van de casus", zie *Kamerstukken II* 2018/19, 35 242, nr. 3, p. 4 en 5.
13 *Kamerstukken II* 2018/19, 35 242, nr. 3, p. 5.

te zetten.[14] Daarnaast kunnen operationele belangen ertoe leiden dat een bevoegdheid niet zo gericht mogelijk wordt ingezet. Hierbij kan gedacht worden aan het voorkomen van onderkenning op welke gegevens de aandacht van de dienst is gericht. Ook kunnen financiële belangen een rol spelen. Van de dienst mag worden verlangd dat ze de beschikbare financiële middelen op een efficiënte manier besteden. In de motivering bij de toestemmingsaanvraag zal overtuigend moeten worden uitgelegd waarom de bevoegdheid *niet* zo gericht mogelijk kan worden ingezet en waarom het gerechtvaardigd is dat er ook meer gegevens kunnen worden verzameld, die niet noodzakelijk zullen zijn voor het onderzoek zelf. In de toestemmingsaanvraag zal dan ook moeten worden beschreven welke maatregelen worden genomen ter bescherming van die gegevens die niet inhoudelijk noodzakelijk zijn voor het onderzoek.[15]

In de praktijk bereiken de diensten deze gerichtheid voor wat betreft de interceptie en opslag van gegevens op drie manieren: (1) de keuze voor de communicatiedrager, (2) de keuze voor de gegevensstroom en (3) verdere positieve en negatieve filtering.

Keuze van de communicatiedrager
In de praktijk kiezen de diensten allereerst een communicatiedrager (zoals een kabel of satelliet) die naar verwachting informatie bevat die voor de uitvoering van de onderzoeksopdrachten door de diensten van belang is. Het fysieke ontvangstpunt bij een aanbieder van een communicatiedienst waar de diensten de geïntercepteerde gegevens ontvangen, wordt een accesslocatie genoemd.

Keuze van de gegevensstromen
Binnen de fibers van een kabel zijn 'tientallen' kanalen te onderscheiden. Door de wetgever is beschreven dat de diensten kiezen voor gegevensstromen (en dus kanalen), waarvan de gerede verwachting bestaat dat ze relevant zijn voor het beantwoorden van de onderzoeksopdrachten van de diensten.

Het toepassen van filters
Niet alle opgevangen gegevensstromen worden ook voor verdere verwerking opgeslagen. Kort na de daadwerkelijke interceptie van gegevens vindt namelijk filtering plaats.[16] Filteren is het proces waarbij op basis van (technische) kenmerken zoals een IP-adres, taal of een e-mailadres wordt bepaald of gegevens al dan niet worden opgeslagen. Een positief filter houdt in dat gegevens worden opgeslagen als zij *matchen* met het betreffende kenmerk. Bij negatieve filtering worden gegevens juist niet opgeslagen.

Datareductie en relevantie (artikel 27)

De verplichting tot datareductie voor kabelinterceptie vloeit voort uit artikelen 27 en 48 lid 5. Deze bepalingen houden – kort gezegd – in dat de hoeveelheid van gegevens die door middel van kabelinterceptie worden verzameld zo snel mogelijk moet worden gereduceerd tot alleen potentieel relevante gegevens.

In algemene zin geldt dat nadat de gegevens eenmaal zijn geïntercepteerd en opgeslagen, de gegevens dienen te worden beoordeeld op relevantie, zodat uiteindelijk alleen relevante gegevens overblijven.[17] De relevantiebeoordeling dient binnen een bepaalde termijn plaats te vinden, dit is de zogeheten

14 *Kamerstukken II* 2018/19, 35 242, nr. 3, p. 5.
15 *Kamerstukken II* 2018/19, 35 242, nr. 3, p. 6 en 7.
16 Het toepassen van filters is onderdeel van de interceptiebevoegdheid van artikel 48.
17 De wettekst van artikel 27 lid 1 Wiv 2017 beschrijft dat sprake is van relevantie wanneer de gegevens relevant zijn voor het onderzoek waarvoor ze zijn verworven, dan wel voor enig ander lopend onderzoek dat valt onder de taken als bedoeld in artikel 8 lid 2 onder a en d, dan wel artikel 10 lid 2 onder a, c en e Wiv 2017. De nota naar aanleiding van het verslag voegt hieraan toe dat de toets op relevantie een inhoudelijke toets is "waarbij onder meer wordt gekeken of de gegevens in positieve zin bijdragen aan het onderzoek, alsook of die gegevens bepaalde vragen negatief kunnen beantwoorden, hypothesen kunnen ontkrachten of anderszins van doorslaggevend belang zijn", zie *Kamerstukken II*, 2016-17, 34 588, nr. 18, p. 32.

'bewaartermijn'. Deze bewaartermijn begint te lopen vanaf het moment dat de gegevens geïntercepteerd zijn. De bewaartermijn voor gegevens uit kabelinterceptie is een jaar (artikel 4 Beleidsregels Wiv 2017). Deze bewaartermijn mag maximaal twee keer met een jaar worden verlengd.[18] Voor een verlenging van de bewaartermijn moet de minister, of namens deze het hoofd van de dienst, toestemming geven. Het verzoek tot verlenging hoeft niet aan de TIB te worden voorgelegd. Gegevens die met kabelinterceptie zijn verzameld mogen dus maximaal drie jaar worden bewaard. Voor geïntercepteerde gegevens die zijn versleuteld geldt dat deze gegevens drie jaar mogen worden bewaard en dat deze termijn telkens met drie jaar mag worden verlengd. Het vereiste uit artikel 27 lid 1 dat de relevantiebeoordeling 'zo spoedig mogelijk' moet gebeuren, geldt niet voor gegevens die door middel van kabelinterceptie zijn verworven.[19] Dit betekent volgens de wetgever echter niet dat de gegevens gedurende de gehele drie jaar worden bewaard. Op grond van artikel 18 dienen de diensten zo snel mogelijk tot datareductie te komen om de inbreuk die (mogelijk) wordt gemaakt op de persoonlijke levenssfeer van burgers zo beperkt mogelijk te houden.[20]

Taakuitvoering (artikel 28 Wiv)

Artikel 28 lid 1 bepaalt dat een bijzondere bevoegdheid slechts mag worden uitgeoefend voor zover dat noodzakelijk is voor de goede uitvoering van de taken van de AIVD, zoals bedoeld in artikel 8 lid 2 onder a en d, en van de MIVD, zoals bedoeld in artikel 10 lid 2 onder a, c en e.[21] Concreet betekent dit dat de bevoegdheden uit artikel 48, 49 lid 1, 52 en 53 alleen mogen worden ingezet voor onderstaande taken:

- Het verrichten van onderzoek met betrekking tot organisaties en personen die door de doelen die zij nastreven, dan wel door hun activiteiten aanleiding geven tot het ernstige vermoeden dat zij een gevaar vormen voor het voortbestaan van de democratische rechtsorde, dan wel voor de veiligheid of voor andere belangen van de staat (AIVD) (artikel 8, lid 1 sub a);
- Het verrichten van onderzoek betreffende andere landen (AIVD) (artikel 8, lid 1 sub d);
- Het verrichten van onderzoek omtrent het potentieel en de strijdkrachten van andere mogendheden ten behoeve van een juiste opbouw en een doeltreffend gebruik van de krijgsmacht (MIVD) (artikel 10 lid 2 sub a);
- Het verrichten van onderzoek naar factoren die van invloed zijn of kunnen zijn op de handhaving en bevordering van de internationale rechtsorde voor zover de krijgsmacht daarbij is betrokken of naar verwachting betrokken kan worden (MIVD) (artikel 10 lid 2 sub a);
- Het verrichten van onderzoek dat nodig is voor het treffen van maatregelen ter voorkoming van activiteiten die ten doel hebben de veiligheid of paraatheid van de krijgsmacht te schaden krijgsmacht (MIVD) (artikel 10 lid 2 sub c);
- Het verrichten van onderzoek dat nodig is voor het treffen van maatregelen ter bevordering van een juist verloop van mobilisatie en concentratie der strijdkrachten (MIVD) (artikel 10 lid 2 sub c);
- Het verrichten van onderzoek betreffende andere landen, ten aanzien van onderwerpen met een militaire relevantie (MIVD) (artikel 10 lid 2 sub e).

Vereisten toestemming (artikel 29)

Het verzoek om toestemming en de verlenging van een toestemming dient door de dienst te worden gemotiveerd. In artikel 29 is vastgelegd aan welke eisen dit verzoek moet voldoen. Daarnaast geldt op grond van artikel 5 van de Beleidsregels Wiv 2017 de aanvullende motivering voor het criterium 'zo gericht mogelijk' (zie paragraaf 3.3). Dit betekent dat het verzoek onderstaande elementen moet bevatten:

---

18 Dit is een andere termijn dan de bewaartermijn die geldt voor gegevens die met behulp van andere bijzondere bevoegdheden zijn verzameld. Voor deze gegevens geldt een bewaartermijn van één jaar (artikel 27 lid 1 Wiv 2017).
19 *Kamerstukken II* 2016/2017, 34588, nr. 3, p. 102.
20 *Kamerstukken II* 2018/19, 35 242, nr. 3, p. 102.
21 De bevoegdheid mag niet worden ingezet ten behoeve van het verrichten van veiligheidsonderzoeken (de zogenoemde B-taak).

- Een aanduiding van de bevoegdheid waarvoor toestemming wordt gevraagd;
- Voor zover van toepassing, de identiteit van de persoon dan wel de organisatie waarvan de uitoefening van de bevoegdheid wordt verlangd;
- Voor zover de betrokkene werkzaam is als journalist of advocaat, de vermelding van deze hoedanigheid;
- Een omschrijving van het onderzoek waarvoor de bevoegdheid wordt ingezet;
- Een omschrijving van het beoogde doel;
- De reden waarom uitoefening van de bevoegdheid noodzakelijk wordt geacht. Hier zullen ook de afwegingen met betrekking tot de eisen van proportionaliteit en subsidiariteit hun beslag dienen te krijgen;
- Motivering op welke wijze de bevoegdheid zo gericht mogelijk wordt ingezet;
- Indien sprake is van een verlenging, een aanduiding van de met de uitoefening behaalde resultaten;
- De beschrijving voor welk onderzoek en voor welk doel de bevoegdheid wordt ingezet, mag geen globale beschrijving zijn, maar moet zo concreet mogelijk worden omschreven.

Aantekening houden (artikel 31 Wiv 2017)

Artikel 31 Wiv 2017 bepaalt dat van de uitoefening van een bevoegdheid voor het verzamelen van gegevens aantekening dient te worden gehouden. De wijze van verslaglegging laat de wetgever open. Hierdoor zijn ook andere vormen dan schriftelijke vastlegging mogelijk. Geautomatiseerde vastlegging (logging) kan als vorm dienen voor het bijhouden van een verslag. [22]

Tussenconclusie

Voor het operationaliseren van de accesslocatie en het uitvoeren van de interceptie gelden in ieder geval onderstaande algemene bepalingen uit de Wiv 2017:

- De verwerking van gegevens mag slechts plaatsvinden voor een bepaald doel en voor zover dat noodzakelijk (alsmede proportioneel en subsidiair) is;
- Er dienen zodanige technische, personele en organisatorische maatregelen te zijn ingericht dat de diensten voortdurend in controle zijn op de wijze waarop de gegevens worden verwerkt en adequate controle en effectief toezicht mogelijk is (zorgplicht);
- De uitoefening van de bevoegdheid dient evenredig te zijn met het daarmee beoogde doel (proportionaliteitsvereiste);
- Gekozen dient te worden voor de minst ingrijpende bevoegdheid (subsidiariteitsvereiste);
- De bevoegdheid dient zo gericht mogelijk te worden ingezet;
- De diensten dienen zo snel mogelijk tot datareductie te komen om de inbreuk die (mogelijk) wordt gemaakt op de persoonlijke levenssfeer van burgers zo beperkt mogelijk te houden;
- Gegevens die niet op relevantie zijn beoordeeld worden meteen vernietigd bij het verstrijken van de bewaartermijn;
- De geïntercepteerde gegevens die niet relevant zijn, moeten meteen worden vernietigd;
- De inzet van de bevoegdheid dient noodzakelijk te zijn voor de taakuitvoering;
- Het verzoek om toestemming dient te voldoen aan de gestelde eisen;
- Van de uitoefening van een bevoegdheid voor het verzamelen van gegevens dient aantekening te worden gehouden.

22 Zie ook *Kamerstukken II* 2016/17, 35488, nr. 3, p. 50.

3. Operationaliseren van de accesslocatie

Dit hoofdstuk beschrijft de specifieke verplichtingen voor de diensten die zijn vastgelegd in artikel 52 (informatieplicht) en artikel 53 (medewerkingsplicht).

Om op een goede wijze uitvoering te kunnen geven aan kabelinterceptie is informatie en medewerking van de aanbieder van de communicatiedienst essentieel. Dit is anders in het geval van etherinterceptie. Voor deze vorm van interceptie beschikt de dienst (onder meer) over een eigen satellietgrondstation. Artikel 52 geeft de diensten de bevoegdheid om aan een aanbieder van een communicatiedienst de opdracht te geven informatie te verstrekken die noodzakelijk is om uitvoering te kunnen geven aan het intercepteren. In de memorie van toelichting wordt toegelicht dat artikel 52 een tweeledig doel heeft. Enerzijds biedt deze bevoegdheid voor de diensten een mogelijkheid om het communicatielandschap in kaart te brengen om vervolgens de interceptiebevoegdheid van artikel 48 'doelgericht' te kunnen inzetten.[23] Anderzijds kunnen de diensten met deze bevoegdheid informatie opvragen om een verzoek voor de inzet van artikel 48 (interceptie) en de daarvoor benodigde medewerking op basis van artikel 53 nader te motiveren.

Artikel 53 regelt de bevoegdheid voor de diensten om aan de betreffende aanbieder van de communicatiedienst opdracht te geven tot medewerking van het uitvoeren van kabelinterceptie. De inzet van deze bevoegdheid is gekoppeld aan de inzet van de interceptie uit artikel 48. Dit betekent dat de medewerkingsplicht alleen kan worden ingezet als toestemming is verkregen voor de inzet van de interceptie. De aanbieders zijn verplicht om aan het verzoek tot medewerking te voldoen. Het niet voldoen aan een dergelijk verzoek is strafbaar (artikel 143). De wetgever heeft gekozen voor een plicht, aangezien in gevallen waarbij de nationale veiligheid in het geding is de diensten niet afhankelijk dienen te zijn van vrijwillige medewerking.

Het te beschermen belang van de artikelen 52 en 53 verschilt van veel andere bijzondere bevoegdheden van de diensten. Waar de andere bevoegdheden veelal een inbreuk op de grondrechten van burgers normeren, wordt in artikelen 52 en 53 een plicht voor marktpartijen in het leven geroepen. Het te beschermen belang betreft dan ook de belangen, rechten en plichten van deze private marktpartijen. Hierbij kan gedacht worden aan het beschermen van bedrijfsgevoelige gegevens, het waarborgen van de continuïteit van de dienstverlening van de aanbieder of aan het feit dat een aanbieder kosten maakt om te voldoen aan de informatie- en medewerkingsplicht.

Aard van de informatie informatieplicht

In het Besluit gegevensverstrekking onderzoek van communicatie Wiv 2017 is geregeld welke informatie kan worden opgevraagd ten behoeve van de inzet van de kabelinterceptie.[24] Het gaat onder meer om de technische gegevens van bijvoorbeeld het door de desbetreffende aanbieder geëxploiteerde telecommunicatienetwerk of dienst. Ook kan informatie worden gevraagd om te kunnen bepalen welke technische voorzieningen er getroffen dienen te worden om daadwerkelijk kabelinterceptie te kunnen toepassen.

Daarnaast kan het gaan om gegevens die bij kunnen dragen aan het in kaart brengen van het communicatielandschap. Om doelgericht te kunnen intercepteren dient inzichtelijk te zijn waar welke soort communicatie wordt verwerkt c.q. getransporteerd. Het betreft hier bijvoorbeeld informatie over zakelijke klanten/(ver)huurders van de aanbieder van de communicatiediensten en de bekende gegevens over de aangeboden diensten en karakteristieken van verkeersstromen.[25] Dit inzicht kan

23 *Kamerstukken II* 2016/17, 34588, nr. 3, p. 113 e.v.
24 *Stb*. 2018, 116.
25 *Kamerstukken II* 2016/17, 34588, nr. 3, p. 114.

deels worden verkregen door de inzet van *search* gericht op interceptie. Een deel van de informatie kan echter uitsluitend van de desbetreffende aanbieders zelf worden verkregen.

Toestemming

Voor het inzetten van de informatieplicht is geen ministeriële toestemming vereist. De opdracht wordt schriftelijk door het hoofd van de dienst verleend. De wetgever geeft hiervoor als reden dat het niet gaat om gegevens waarbij de persoonlijke levenssfeer van concrete personen in het geding is. Het gaat hierbij immers voornamelijk om technische en bedrijfsmatige gegevens. De wet kent daarnaast geen maximale duur waarvoor de informatieplicht mag worden ingezet. Op grond van artikel 29 mag een toestemming voor de uitoefening van een bijzondere bevoegdheid als bedoeld in paragraaf 3.2.5. van de Wiv 2017 worden verleend voor een periode van ten hoogste drie maanden. Artikel 52 is een bijzondere bevoegdheid uit paragraaf 3.2.5. Er is hier echter geen sprake van het verlenen van toestemming, maar van het geven van een opdracht door het hoofd van de dienst aan een aanbieder om gegevens te verstrekken.

In tegenstelling tot artikel 52 geldt dat voor de inzet van de medewerkingsplicht toestemming benodigd is van de betrokken minister. De toestemming wordt verleend voor een periode van ten hoogste een jaar en kan steeds met eenzelfde periode worden verlengd. Het verzoek om toestemming dient te worden gedaan door het hoofd van de dienst aan de minister. Nadat de minister toestemming heeft verleend, zal de TIB de rechtmatigheid van de verleende toestemming toetsen. In artikel 29 is vastgelegd aan welke eisen een verzoek aan toestemming moet voldoen (zie hoofdstuk 2). Daarnaast zijn in artikel 53 twee aanvullende voorwaarden opgenomen waaraan het toestemmingsverzoek moet voldoen, namelijk om welke aanbieder het precies gaat en een omschrijving van de medewerking die van de aanbieder wordt verwacht.

Overleg voorafgaand aan het inzetten van de medewerkingsplicht

Nadat toestemming is verleend voor de inzet van de medewerkingsplicht, dienen de diensten eerst overleg te voeren met de betreffende aanbieder. Het voorgeschreven nader overleg met de aanbieder is onder meer bedoeld om de praktische invulling van de medewerking te bespreken, hierbij valt te denken aan de precieze specificaties van de technische voorzieningen. Ook kan over andersoortige aangelegenheden worden gesproken, zoals de implementatietermijn en eventuele personele en organisatorische aspecten die zijn verbonden aan de uitvoering van de verleende toestemming.[26] Pas na dit overleg zal de daadwerkelijke medewerking aanvangen en kunnen er technische maatregelen worden genomen om de interceptie te realiseren. Als sprake is van een verlenging hoeft dit overleg niet opnieuw te worden gevoerd.

In stand houden van de technische voorziening

Indien op enig moment het niet meer noodzakelijk is om bij de desbetreffende aanbieder telecommunicatie te intercepteren, zijn de diensten bevoegd om de getroffen technische voorzieningen bij de aanbieder in stand te laten. Dit kan bijvoorbeeld het geval zijn als sprake is van een wijziging in de onderzoeksopdrachten van de diensten. De getroffen voorzieningen mogen op grond van artikel 53 lid 6 tot een jaar na afloop van de toestemmingsperiode in stand worden gehouden. De wetgever geeft hiervoor als reden dat de uitvoering van de interceptiebevoegdheid bij de desbetreffende aanbieder maatwerk is. Dit vereist niet alleen de nodige implementatietijd, maar ook de nodige investeringen. Als binnen dit jaar het nodig is om opnieuw de medewerking van de desbetreffende aanbieder in te roepen, dan kan deze op korte termijn worden gerealiseerd. Indien het in stand houden van de technische voorzieningen geen doel meer dient, dan is het mogelijk om de aanbieder te ontheffen van zijn verplichtingen.[27]

26 *Kamerstukken II* 2016/17, 34588, nr. 3, p. 116.
27 Artikel 53 lid 6 Wiv 2017.

Tussenconclusie

Naast de verplichtingen die gelden vanuit de algemene bepalingen uit de Wiv 2017, voegt artikel 52 onderstaande specifieke verplichtingen toe die gelden voor de inzet van de bevoegdheid van de informatieplicht:

- De opgevraagde gegevens dienen te vallen onder het Besluit gegevensverstrekking onderzoek van communicatie Wiv 2017;
- Voor de inzet van informatieplicht dient er toestemming te zijn van het hoofd van de dienst;
- Voor de inzet van de medewerkingsplicht dient er toestemming te zijn van de minister. Deze toestemming wordt getoetst op rechtmatigheid door de TIB;
- De toestemming voor het inzetten van de medewerkingsplicht kan steeds voor maximaal een jaar worden verleend;
- De inhoud van het verzoek om toestemming voor de inzet van de medewerkingsplicht voldoet aan de hiervoor gestelde eisen;
- Indien de medewerking niet meer noodzakelijk is, mogen de getroffen voorzieningen voor maximaal een jaar in stand blijven. Indien het in stand houden geen doel meer dient wordt de aanbieder ontheven van zijn verplichting.

4. Uitvoeren van kabelinterceptie

Dit hoofdstuk beschrijft de specifieke wettelijke verplichtingen die gelden voor de uitvoering van de kabelinterceptie. Zoals in het rapport beschreven heeft in de onderzoeksperiode een beperkte vorm van interceptie plaatsgevonden, namelijk het snapshotten. Het snapshotten kent geen wettelijke grondslag in de Wiv, maar wordt uitgevoerd op grond van artikel 48 (kabelinterceptie). De opgeslagen gegevens worden vervolgens onderzocht op grond van artikel 49 lid 1 (*search* gericht op interceptie) met als doel het vaststellen van de potentiële inlichtingenwaarde van de gegevens.

Toestemming

Voor het uitoefenen van de bevoegdheid tot kabelinterceptie en *search* gericht op interceptie is toestemming vereist van de betrokken minister.[28] Vanwege de nauwe samenhang tussen de bevoegdheid tot interceptie en de bevoegdheid tot *search* gericht op interceptie, ligt het voor de hand dat vaak sprake zal zijn van een 'combinatieaanvraag', waarin voor beide bevoegdheden toestemming zal worden verzocht. Nadat de minister toestemming heeft verleend, toetst de TIB de rechtmatigheid van de toestemming. De toestemming wordt verleend voor een periode van maximaal een jaar en kan telkens met een jaar worden verlengd. De wetgever heeft hiermee afgeweken van de reguliere termijn van drie maanden. Hiervoor is gekozen omdat de indringendheid van de privacy-inbreuk in deze fase beperkt is.[29] In deze fase mag de inhoud van de gegevens namelijk alleen om technische redenen worden bekeken.

Inhoud toestemmingsverzoek

Naast de algemene vereisten uit artikel 29 die voor de inhoud van een toestemmingsverzoek gelden (zie hoofdstuk 2), gelden voor kabelinterceptie twee aanvullende vereisten. Uit artikel 48 lid 3 volgt dat als naast de metadata ook inhoud wordt geïntercepteerd, dit extra dient te worden gemotiveerd.

Ook moet in het verzoek een typering worden gegeven van de telecommunicatie of de gegevensoverdracht door middel van een geautomatiseerd werk, waarvoor de bevoegdheid dient te worden ingezet. Er moet duidelijk zijn omschreven om welk type interceptie het gaat, bijvoorbeeld van de kabel of ether. Indien mogelijk moet de aard van de communicatie (bijvoorbeeld GSM-radio- of internetverkeer) worden beschreven al dan niet met een geografische afbakening. Ook dienen de diensten waar mogelijk op te nemen welke soorten verkeer relevant zijn, zoals spraak, chatverkeer of bestandsuitwisseling. Als laatste dient nader te worden aangegeven om welk deel van de kabelinfrastructuur het gaat en wat voor soort verkeer dient te worden geïntercepteerd.[30]

Specifiek doel voor verwerken van de gegevens

Gegevens die zijn geïntercepteerd mogen alleen worden verwerkt voor de doelen zoals die zijn genoemd in artikel 48 en 49 lid 1. De diensten mogen op grond van artikel 48 technische analyse uitvoeren ter optimalisatie van de inzet van de interceptiebevoegdheid. Ook het raadplegen van inhoud is voor dat doel toegestaan. Met inhoud wordt hier gedoeld op de inhoud van communicatie (zoals de tekst van een e-mail) in tegenstelling tot verkeersgegevens, oftewel metadata (wie communiceert met wie, bijvoorbeeld de afzender en ontvanger van een e-mail).

28 Artikel 48 lid 2 Wiv 2017.
29 *Kamerstukken II* 2016/2017, 34588, nr. 3, p. 99.
30 Artikel 48 lid 3 Wiv 2017 en *Kamerstukken II* 2016/2017, 34588, nr. 3, p. 99.

Op grond van artikel 49 lid 1 (*search* gericht op interceptie) mogen de diensten de gegevens onderzoeken met het oog op:

- het vaststellen van de kenmerken en de aard van de telecommunicatie;
- het vaststellen van de identiteit van de persoon of organisatie behorende bij de telecommunicatie.

Kortom, met deze bevoegdheid kunnen de diensten vaststellen of zij daadwerkelijk datgene intercepteren dat wordt beoogd.

De inhoud van de geïntercepteerde gegevens mag dus alleen worden bekeken met als doel het optimaliseren van de interceptie. Als de dienst constateert dat het gebruik van de inhoud van de communicatie noodzakelijk is voor de goede taakuitvoering, dan dient een verzoek om toestemming te worden ingediend voor artikel 47 (gerichte interceptie) of artikel 50 (selectie).[31]

Functie- en taakscheiding

De verschillende fases in het interceptieproces dienen een specifiek doel. Zowel in artikel 48 als in artikel 49 is bepaald dat alleen daartoe aangewezen medewerkers kennis mogen nemen van de verzamelde gegevens voor dit bepaalde doel. Het aanwijzen van de bevoegde medewerkers, bij uitsluiting van anderen, wordt gedaan per besluit van de minister. De minister kan deze bevoegdheid mandateren aan het hoofd van de dienst.[32] Ook voor het voldoen aan de zorgplicht en het algemene vereiste van zorgvuldige gegevensverwerking moet sprake zijn van functie- en taakscheiding. Om functie- en taakscheiding te bewerkstelligen kan gedacht worden aan het digitaal toegang verlenen tot de gegevens door middel van autorisaties, maar ook aan fysieke maatregelen. Bij fysieke maatregelen kan worden gedacht aan compartimentering door middel van het gebruiken van een toegangspas tot de ruimte waarin de gegevens worden verwerkt en het voorkomen wordt dat mee kan worden gekeken op een scherm.[33]

Alleen de aangewezen medewerkers mogen kennisnemen van de geïntercepteerde gegevens. Zij mogen dit voor artikel 48 alleen doen met het doel te waarborgen en te controleren dat gegevens goed worden ontvangen en kunnen worden opgeslagen. Bij het controleren op een juiste ontvangst kan worden gedacht aan het ordenen en labelen van gegevens of het controleren op ruis.[34] Ook mogen deze medewerkers de gegevens, indien mogelijk, ontsleutelen. Als de gegevens eenmaal ontsleuteld zijn, mag van de inhoud van de communicatie kennis worden genomen, maar uitsluitend voor het beschreven doel van artikel 48.

Voor artikel 49 lid 1 geldt dat alleen daartoe aangewezen ambtenaren kennis mogen nemen van de verzamelde gegevens met als doel het optimaliseren van de interceptie en om de vraag te kunnen beantwoorden of datgene wordt geïntercepteerd wat beoogd was.

Aantekening houden

Uit artikel 49 lid 3 volgt dat de diensten, wanneer dit noodzakelijk is voor een goede taakuitvoering, aantekening mogen houden van de resultaten van de toepassing van *search* gericht op interceptie. Deze vorm van aantekening staat los van de wettelijke verplichting van het aantekening houden (artikel 31) van de inzet van de bevoegdheid uit artikel 49 lid 1. De verkenning van gegevens kan tot een bepaald beeld van de gegevensstroom of van 'het communicatielandschap' leiden, wat voor toekomstige activiteiten aanknopingspunten kan bieden. Hierbij valt te denken aan de analyses waaruit blijkt dat een bepaalde fiber geen relevante gegevens bevat en daardoor niet 'in interceptie'

31 *Kamerstukken II* 2016/2017, 34588, nr. 3, p. 107.
32 Artikel 48 lid 4 Wiv 2017.
33 In CTIVD-rapport nr. 70, p. 28, benadrukt de CTIVD dat ook fysieke afstand onderdeel is van de waarborgfunctie van het systeem van functie- en taakscheiding.
34 *Kamerstukken II* 2016/2017, 34588, nr. 3, p. 97 en 98.

moet worden gehouden. In een dergelijke analyse zou kunnen staan wat voor soort gegevens over de kabel worden verzonden en welke personen en/of organisaties over het algemeen van deze fiber gebruikmaken. De resultaten van dergelijke analyses kunnen verder worden gebruikt voor het doel waarvoor deze zijn opgetekend. Dit betekent niet dat iedere medewerker kennis mag nemen van deze resultaten. Uitsluitend medewerkers die in het kader van de aan hen opdragen taakuitvoering kennis moeten nemen van de resultaten zijn hiertoe gerechtigd.[35] Hierbij kan het ook gaan om medewerkers die werkzaam zijn in het inlichtingenproces en kennis moeten kunnen nemen van de aantekening, bijvoorbeeld ten behoeve van het opstellen van een nieuw verzoek om toestemming.

Geen verder onderzoek op inhoud in de fase van *searchen*

De inhoud van de geïntercepteerde gegevens mag in deze fase alleen worden bekeken met als doel het optimaliseren van de interceptie. Als de dienst constateert dat het gebruik van de inhoud van de communicatie noodzakelijk is voor de goede taakuitvoering, dan dient een verzoek om toestemming te worden ingediend voor artikel 47 (gerichte interceptie) of artikel 50 (selectie).[36]

In de toelichting op de wet wordt beschreven dat targets uitwijken naar open en anonieme opstijgpunten van het internet (zoals wifi-netwerken in hotels, restaurants en andere openbare ruimtes) waardoor een gerichte tap bij de traditionele aanbieders van telecommunicatiediensten in Nederland steeds minder effectief is en onderzoeksopdrachtgerichte interceptie noodzakelijk is.[37] Als echter bij het *searchen* wordt gestuit op het target, kan het zijn dat een gerichte tap wel mogelijk wordt en moet een afweging worden gemaakt in het kader van gerichtheid en subsidiariteit of art. 47 moet worden ingezet.

Het kan volgens de wetgever voorkomen dat de dienst in de fase van *search* gericht op interceptie stuit op gegevens van nieuwe personen of organisaties die in aanmerking komen voor onderzoek door de dienst. In een dergelijk geval kan de dienst een toestemmingsaanvraag doen voor het selecteren van de gegevens (artikel 50 lid 1 sub a).[38]

Bestemming en herkomst Nederland

In de begeleidende brief bij de Beleidsregels Wiv 2017 hebben de ministers van BZK en Defensie de toezegging gedaan dat het vrijwel uitgesloten is dat kabelinterceptie de komende jaren wordt ingezet voor onderzoek naar communicatie met oorsprong en bestemming in Nederland.[39] De gedachte hierachter is dat in dergelijke situaties een gerichter middel kan worden ingezet, bijvoorbeeld een gerichte tap. Andere landen die kabelinterceptie toepassen, hebben veelal een soortgelijke uitzondering. Op deze toezegging is de uitzondering gemaakt voor onderzoek naar *cyber defence*. De minister geeft hiervoor als reden dat bij digitale aanvallen misbruik wordt gemaakt van de Nederlandse digitale infrastructuur en kabelinterceptie noodzakelijk kan zijn om dit te onderkennen.

Op het moment dat de toezegging werd gedaan speelde in het maatschappelijk debat de vraag of de diensten, dankzij de nieuwe bevoegdheid van kabelinterceptie, hele woonwijken zouden kunnen gaan aftappen waardoor willekeurige Nederlanders in 'het sleepnet' terecht zouden kunnen komen. Met deze toezegging lijken de ministers de hiervoor genoemde aanname uit de wereld te willen helpen. Desondanks is het onduidelijk wat de toezegging in de praktijk precies inhoudt en welk(e) belang(en) deze dient. De vraag is of de toezegging ten doel heeft Nederlandse staatsburgers te beschermen of alle personen die zich in Nederland bevinden. Dat laatste heeft als gevolg dat kabelinterceptie niet is

35 *Kamerstukken II* 2016/2017, 34588, nr. 3, p. 104.
36 *Kamerstukken II* 2016/2017, 34588, nr. 3, p. 107.
37 *Kamerstukken II* 2016/2017, 34588, nr. 3, p. 92.
38 In de onderzoeksperiode is in de verzoeken om toestemming opgenomen dat de gegevens niet mogen worden gebruikt door het inlichtingenproces.
39 *Kamerstukken II* 2017/18, 34588, nr. 76.

toegestaan voor communicatie van buitenlandse targets die zich (tijdelijk) in Nederland bevinden als de communicatie ook Nederland als bestemming heeft.

Bewaartermijnen

De bewaartermijn voor gegevens uit kabelinterceptie is een jaar (artikel 4 Beleidsregels Wiv 2017). Deze bewaartermijn mag maximaal twee keer met een jaar worden verlengd.[40] De diensten zullen in het verzoek om toestemming dienen aan te tonen waarom de desbetreffende gegevens nog voor een periode van een jaar dienen te worden bewaard. Voor een verlenging van de bewaartermijn moet de minister, of namens deze het hoofd van de dienst, toestemming geven. Het verzoek tot verlenging hoeft niet aan de TIB te worden voorgelegd, zoals dat geldt voor de bevoegdheden waar de TIB een rol speelt. Gegevens die met kabelinterceptie zijn verzameld, mogen dus maximaal drie jaar worden bewaard. Voor geïntercepteerde gegevens die zijn versleuteld, geldt dat deze gegevens drie jaar mogen worden bewaard en dat deze termijn telkens met drie jaar mag worden verlengd.

Tussenconclusie

Naast de verplichtingen die gelden vanuit de algemene bepalingen uit de Wiv 2017, voegt artikel 48 onderstaande specifieke verplichtingen toe die gelden voor de inzet van de bevoegdheid tot kabelinterceptie:

- Voor de inzet van kabelinterceptie en *search* gericht op interceptie dient toestemming te worden verleend door de betreffende minister;
- De toestemming van de minister moet door de TIB op rechtmatigheid worden getoetst;
- De toestemming voor de inzet van kabelinterceptie en *search* gericht op interceptie wordt voor maximaal een jaar verleend;
- De gegevens mogen alleen worden verwerkt ten behoeve van de doelen zoals genoemd in artikel 48 en 49 lid 1;
- Er is sprake van functie- en taakscheiding bij het verwerken van de geïntercepteerde gegevens;
- De betreffende medewerkers dienen te zijn aangewezen;
- Van de resultaten van het onderzoek op basis van artikel 49 lid 1 mag aantekening worden gehouden;
- De bevoegdheid tot kabelinterceptie wordt niet ingezet voor onderzoek naar communicatie met bestemming en herkomst Nederland, behalve als het gaat om onderzoek in het kader van *cyber defence*;
- Gegevens die door middel van kabelinterceptie zijn verworven, mogen maximaal een jaar worden bewaard. Deze termijn mag met maximaal twee keer met één jaar worden verlengd. De verlenging dient te worden gemotiveerd. De minister, of namens deze het hoofd van de dienst, dient toestemming te geven;
- Versleutelde gegevens mogen maximaal 3 jaar worden bewaard. Zolang de gegevens niet ontsleuteld zijn mag deze termijn met telkens 3 jaar worden verlengd. Hiervoor moet toestemming worden gegeven door de minister of namens deze het hoofd van de dienst.

40 Dit is een andere termijn dan de bewaartermijn die geldt voor gegevens die met behulp van andere bijzondere bevoegdheden zijn verzameld. Voor deze gegevens geldt een bewaartermijn van één jaar (artikel 27 lid 1 Wiv 2017).

5. Cyber defence

De minister van BZK en de minister van Defensie hebben in hun brief van 25 april 2018 toegezegd dat het vrijwel uitgesloten is dat kabelinterceptie de komende jaren wordt ingezet voor onderzoek naar communicatie met oorsprong en bestemming in Nederland. In hun brief maakten zij op dit punt wel een uitzondering voor onderzoek in het kader van *cyber defence*. De ministers gaven hiervoor als reden omdat bij digitale aanvallen misbruik wordt gemaakt van de Nederlandse digitale infrastructuur en kabelinterceptie noodzakelijk kan zijn om dit te onderkennen.

Onderzoeken op het gebied *cyber defence* kunnen, in tegenstelling tot onderzoeken naar andere onderwerpen, plaatsvinden op basis van artikel 48 en artikel 49 lid 1 Wiv 2017. Dit betekent dat de verzamelde informatie die wordt gebruikt voor *search* gericht op interceptie kan worden gebruikt voor onderzoeken op het gebied van *cyber*. Dergelijke onderzoeken vinden plaats door de inzet van bijvoorbeeld netwerkmonitoring of netwerkdetectie.

Netwerkmonitoring of netwerkdetectie wordt ingezet om afwijkingen in het normale internetverkeer te detecteren. Deze afwijkingen kunnen duiden op bijvoorbeeld een aanval op een server door een statelijke actor, zoals een DDoS-aanval.[41] Een DDoS-aanval is een *cyber*-aanval waarbij zodanig veel internetverkeer naar bijvoorbeeld een server wordt gestuurd, waardoor deze server overvraagd wordt en niet meer benaderbaar is. Om dergelijke aanvallen te herkennen is onderzoek nodig op het Nederlandse netwerk. In de memorie van toelichting is te lezen dat artikel 49 lid 1 sub a Wiv 2017 de mogelijkheid biedt om onderzoek te doen naar kenmerken van ongewenste activiteiten (bijv. *signatures van malware*) en naar verkeer dat ongebruikelijke afwijkingen vertoont (anomaliedetectie).

Dergelijk onderzoek kan zowel *offline* als *online* plaatsvinden. In het eerste geval wordt een gegevensbestand van geïntercepteerde gegevens gevormd, waarop vervolgens onderzoek plaatsvindt. In het tweede geval wordt *real time* en online het dataverkeer geanalyseerd. De diensten voeren deze zogeheten netwerkmonitoring uit op basis van hun (contra-)inlichtingentaak.[42]

Voor het uitvoeren van netwerkmonitoring of netwerkdetectie geldt dat toestemming van de minister moet worden verkregen, waarbij aan de daaraan gestelde eisen (volgend uit artikelen 29, 48 lid 1 en 49 lid 1 Wiv 2017) moeten worden voldaan. Bij het verzoek om toestemming moet niet alleen zo concreet mogelijk worden aangegeven voor welk onderzoek, welk deel van de kabelgebonden infrastructuur voor welk doel dient te worden onderzocht, maar ook zal duidelijk dienen te worden aangegeven waaruit dat onderzoek precies bestaat. Aangezien de activiteit netwerkmonitoring of netwerkdetectie (artikel 49 lid 1 Wiv 2017) niet zonder de bevoegdheid tot kabelinterceptie op grond van artikel 48 Wiv 2017 kan plaatsvinden, zal ook hier veelal sprake zijn van een combinatie-aanvraag.[43]

41 DDoS staat voor *Distributed Denial of Service* en is een aanval waarbij men probeert een computer, netwerk of dienstverlening (tijdelijk) uit te schakelen.
42 Artikelen 8 lid 2 sub a, onderscheidenlijk artikel 10 lid 2 sub a en c Wiv 2017.
43 *Kamerstukken II* 2016/17, 34588, nr. 3, p. 105.

6. Samenvatting van wettelijke vereisten

Op basis van de wettelijke vereisten komt de CTIVD tot onderstaand toetsingskader voor het toezichtsrapport over de inzet van kabelinterceptie door de AIVD en de MIVD.

Wettelijke vereisten algemene bepalingen

- De verwerking van gegevens mag slechts plaatsvinden voor een bepaald doel en voor zover dat noodzakelijk (alsmede proportioneel en subsidiair) is;
- Er dienen zodanige technische, personele en organisatorische maatregelen te zijn ingericht dat de diensten voortdurend in controle zijn op de wijze waarop de gegevens worden verwerkt en adequate controle en effectief toezicht mogelijk is;
- De uitoefening van de bevoegdheid dient evenredig te zijn met het daarmee beoogde doel (proportionaliteitsvereiste);
- Gekozen dient te worden voor de minst ingrijpende bevoegdheid (subsidiariteitsvereiste);
- De bevoegdheid dient zo gericht mogelijk te worden ingezet;
- De diensten dienen zo snel mogelijk tot datareductie te komen om de inbreuk die (mogelijk) wordt gemaakt op de persoonlijke levenssfeer van burgers zo beperkt mogelijk te houden;
- Gegevens die niet op relevantie zijn beoordeeld, worden meteen vernietigd bij het verstrijken van de bewaartermijn;
- De geïntercepteerde gegevens die niet relevant zijn, moeten meteen worden vernietigd;
- De inzet van de bevoegdheid dient noodzakelijk te zijn voor de taakuitvoering;
- Het verzoek om toestemming dient te voldoen aan de gestelde eisen;
- Van de uitoefening van een bevoegdheid voor het verzamelen van gegevens dient aantekening te worden gehouden.

Wettelijke vereisten operationaliseren accesslocatie

- De opgevraagde gegevens dienen te vallen onder het Besluit gegevensverstrekking onderzoek van communicatie Wiv 2017;
- Voor de inzet van informatieplicht dient er toestemming te zijn van het hoofd van de dienst;
- Voor de inzet van de medewerkingsplicht dient er toestemming te zijn van de minister. Deze toestemming wordt getoetst op rechtmatigheid door de TIB;
- De toestemming voor het inzetten van de medewerkingsplicht kan steeds met maximaal een jaar worden verleend;
- De inhoud van het verzoek om toestemming voor de inzet van de medewerkingsplicht voldoet aan de hiervoor gestelde eisen;
- Indien de medewerking niet meer noodzakelijk is, mogen de getroffen voorzieningen voor maximaal een jaar in stand blijven. Indien het in stand houden geen doel meer dient, wordt de aanbieder ontheven van zijn verplichting.

Wettelijke vereisten uitvoeren kabelinterceptie

- Voor de inzet van kabelinterceptie en *search* gericht op interceptie dient toestemming te worden verleend door de betreffende minister;
- De toestemming van de minister moet door de TIB op rechtmatigheid worden getoetst;
- De toestemming voor de inzet van kabelinterceptie en *search* gericht op interceptie wordt voor maximaal een jaar verleend;
- De gegevens mogen alleen worden verwerkt ten behoeve van de doelen zoals genoemd in artikel 48 en 49 lid 1;
- Er is sprake van functie- en taakscheiding bij het verwerken van de geïntercepteerde gegevens;
- De betreffende medewerkers dienen te zijn aangewezen;
- Van de resultaten van het onderzoek op basis van artikel 49 lid 1 mag aantekening worden gehouden;

- De bevoegdheid tot kabelinterceptie wordt niet ingezet voor onderzoek naar communicatie met bestemming en herkomst Nederland, behalve als het gaat om onderzoek in het kader van *cyber defence*;
- Gegevens die door middel van kabelinterceptie zijn verworven, mogen maximaal een jaar worden bewaard. Deze termijn mag met maximaal twee keer met één jaar worden verlengd. De verlenging dient te worden gemotiveerd. De minister, of namens deze het hoofd van de dienst, dient toestemming te geven;
- Versleutelde gegevens mogen maximaal 3 jaar worden bewaard. Zolang de gegevens niet ontsleuteld zijn, mag deze termijn met telkens 3 jaar worden verlengd. Hiervoor moet toestemming worden gegeven door de minister of namens deze het hoofd van de dienst.

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

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