COMMISSIE VAN TOEZICHT
BETREFFENDE
DE INLICHTINGEN- EN VEILIGHEIDSDIENSTEN

TOEZICHTSRAPPORT

inzake
gegevensverwerking op het gebied van telecommunicatie
door de AIVD en de MIVD

CTIVD nr. 38

[5 februari 2014]

COMMISSIE VAN TOEZICHT
BETREFFENDE
DE INLICHTINGEN- EN VEILIGHEIDSDIENSTEN

CTIVD nr. 38

TOEZICHTSRAPPORT

inzake gegevensverwerking op het gebied van telecommunicatiedoor de AIVD en de MIVD

Inhoudsopgave

COMMISSIE VAN TOEZICHT
BETREFFENDE
DE INLICHTINGEN- EN VEILIGHEIDSDIENSTEN

CTIVD nr. 38

BEGRIPPENLIJST

Bij het openbare toezichtsrapport inzake gegevensverwerking op het gebied van telecommunicatie door de AIVD en de MIVD

In deze lijst wordt een aantal begrippen toegelicht zoals deze gebruikt worden in het toezichtsrapport en de juridische bijlage. De Commissie heeft bij de gegeven omschrijvingen geen volledigheid nagestreefd maar gepoogd de lezer een zo concreet mogelijk beeld te geven van de desbetreffende begrippen.

Afdelingshoofd (MIVD)	Functionaris binnen de MIVD die hiërarchisch als volgt is ingebed in de organisatie: directeur, *afdelingshoofd,* bureauhoofd, sectiehoofd.
Agent	Een persoon die gericht door de diensten wordt ingezet om gegevens te verzamelen. Een agent werkt onder aansturing en onder supervisie van de diensten.
Analoge datastroom	Gegevens die zich door middel van een niet digitale verbinding van het ene naar het andere systeem verplaatsen. De analoge stroom bevat telefonie- en faxverkeer die niet via het internet gaat.
Applicatie	Een computerprogramma waarmee bepaalde taken uitgevoerd kunnen worden (bijvoorbeeld Microsoft Word, waarmee tekst verwerkt kan worden). De diensten maken gebruik van applicaties voor bijvoorbeeld de ontsluiting en analyse van gegevens.
Bijzondere bevoegdheid	Een bevoegdheid van de dienst waarin een specifieke inbreuk op de persoonlijke levenssfeer is geregeld, alsmede de voorwaarden waaronder deze mag worden toegepast. De toepassing van een bijzondere bevoegdheid heeft veelal een geheim karakter. De bijzondere bevoegdheden zijn neergelegd in de artikelen 20 t/m 30 van de Wet op de inlichtingen- en veiligheidsdiensten 2002 (bijvoorbeeld tappen en observeren).
Bulkdata	Grote hoeveelheden ruwe gegevens.
Bureauhoofd (MIVD)	Functionaris binnen de MIVD die hiërarchisch als volgt is ingebed in de organisatie: directeur, afdelingshoofd, *bureauhoofd*, sectiehoofd.
Centraal Informatiepunt Onderzoek Telecommunicatie (CIOT)	Een overheidsinstantie die de toegang verzorgt tot bepaalde, in de wet vastgelegde, gebruikersgegevens van telecom- en internetbedrijven (bijvoorbeeld naam, adres, woonplaats, nummer en soort dienst van een gebruiker), ten behoeve van

	opsporings-, inlichtingen- en veiligheidsdiensten.
Communications intelligence (comint)	De gegevens uit sigint die betrekking hebben op de inhoud en de metagegevens communicatie tussen partijen.
Communicatiesessie	De communicatie tussen twee of meer gebruikers op een bepaald moment (bijvoorbeeld het voeren van een (satelliet) telefoongesprek).
Compartimentering	Het in de praktijk brengen van het need to know beginsel uit artikel 35 Wet op de inlichtingen- en veiligheidsdiensten 2002 in de zin dat binnen de AIVD of de MIVD ervoor wordt zorg gedragen dat informatie alleen aan medewerkers verstrekt wordt voor zover dat noodzakelijk is voor een goede uitvoering van de aan hen opgedragen taken.
Cyber	Datgene dat samenhangt met de digitale of virtuele wereld, waaronder het internet.
Data mining	Het op gestructureerde wijze doorzoeken van grote gegevensverzamelingen.
Datastroom	Gegevens die zich door middel van een verbinding van het ene naar het andere systeem verplaatsen.
Digitale datastroom	Gegevens die zich door middel van een internetverbinding van het ene naar het andere systeem verplaatsen. De digitale stroom bevat telefonieverkeer, faxverkeer en ander internetverkeer.
Directeur (AIVD)	Functionaris binnen de AIVD die hiërarchisch als volgt is ingebed in de organisatie: hoofd, *directeur,* unithoofd, teamhoofd.
Directeur (MIVD)	Functionaris die de leiding heeft over de MIVD. Binnen de MIVD is de directeur hiërarchisch als volgt ingebed in de organisatie: *directeur*, afdelingshoofd, bureauhoofd, sectiehoofd.
E-mailaccount	E-mail is elektronisch postverkeer. Een e-mailgebruiker gebruikt een account om e-mails te verzenden en te ontvangen. Een e-mailaccount kan aangevraagd worden bij een Internet Service Provider (bijvoorbeeld KPN) of een andere aanbieder van e-maildiensten (bijvoorbeeld Hotmail of Gmail).
Electronic intelligence (elint)	De gegevens uit sigint afkomstig uit elektronische signalen (radar).
Ether	De ruimte waarin elektromagnetische golven zich verspreiden. In het onderhavige onderzoek gaat het om het verspreiden van satellietsignalen en radiogolven.
FOIP	'Fax over internetprotocol'. Het betreft het versturen van fax via het internetprotocol.
Geautomatiseerd werk	Een inrichting die bestemd is om langs elektronische weg gegevens op te slaan, te verwerken en over te dragen (bijvoorbeeld een computer, een computernetwerk, een

	mobiele telefoon of een server).
Gebruikersgegevens	Ook wel abonneegegevens genoemd. Het gaat om naam, adres, woonplaats, nummer en soort dienst van een gebruiker.
Geëvalueerde gegevens	Gegevens verkregen door middel van de inzet van bijzondere bevoegdheden die op relevantie zijn beoordeeld.
Gegevensverwerking	Het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens (artikel 1, aanhef f, Wet op de inlichtingen- en veiligheidsdiensten 2002).
Gericht intercepteren	Interceptie waarbij van tevoren kan worden aangegeven op welke persoon, organisatie of technisch kenmerk de gegevensverwerving gericht is.
Hacken	Binnendringen in een geautomatiseerd werk om gegevens te achterhalen of wijzigen.
Hoofd (AIVD)	Functionaris die de leiding heeft over de de AIVD. Binnen de AIVD is het hoofd hiërarchisch als volgt ingebed in de organisatie: *hoofd*, directeur, unithoofd, teamhoofd.
IMEI-nummer	Het unieke nummer waarmee een mobiele telefoon is te identificeren.
Informant	Een persoon of instantie tot wie de diensten zich kunnen wenden om gegevens te verzamelen. Een informant wordt niet aangestuurd en wordt geacht vanuit zijn gebruikelijke activiteiten geacht informatie te kunnen verstrekken.
Inlichtingendienst	Een dienst die onderzoek doet naar andere landen om (potentiële) dreigingen voor de eigen nationale veiligheid te onderkennen.
Inlichtingentaak	Het doen van onderzoek naar andere landen (zie artikel 6, tweede lid, aanhef d en artikel 7, tweede lid, aanhef a en e Wet op de inlichtingen- en veiligheidsdiensten 2002).
Interceptie	Het onderscheppen van gegevens.
Internetprotocol (IP)	Een systeem waarmee computernetwerken met elkaar kunnen communiceren (bijvoorbeeld het Hypertext Transfer Protocol (http) regelt de communicatie tussen een webbrowser (programma om internetpagina's te bekijken) en een internetpagina).
IP-adres	Iedere afzonderlijke computer die via IP met andere computers communiceert heeft een uniek adres, het IP-adres. Het IP-adres identificeert de aansluiting van de computer met het internet, vergelijkbaar met een telefoonnummer.
Kabelgebonden communicatie	Communicatie die via een kabel (bijvoorbeeld glasvezel- en koperverbindingen) loopt.

Last	Toestemming voor het uitoefenen van een bijzondere bevoegdheid (voor het uitvoeren van een telefoontap hebben de diensten bijvoorbeeld een last van de minister nodig).
Leads	Een kenmerk (bijvoorbeeld een telefoonnummer) dat wordt gebruikt voor de inzet van de searchbevoegdheid in het kader van ongerichte interceptie (artikel 26 Wet op de inlichtingen- en veiligheidsdiensten 2002).
Metagegevens	Gegevens over communicatie. De metagegevens van een telefoongesprek zijn bijvoorbeeld de betrokken telefoonnummers, de starttijd en de eindtijd van het gesprek en de gegevens van de betrokken telefoonmasten. De term metadata betekent hetzelfde als metagegevens.
Metadata-analyse	Het proces van zoeken naar relevante verbanden en gegevens in een verzameling metagegevens en het combineren van reeds beschikbare gegevens (wat/wie heeft contact waarmee, hoe lang, hoe vaak, waar vandaan, etc.).
Nationale Sigint Organisatie (NSO)	Een gezamenlijke organisatie van de AIVD en de MIVD die verantwoordelijk is voor de technische aspecten van interceptie van niet-kabelgebonden communicatie.
Netwerkanalyse	Het in kaart brengen, onderling combineren en het leggen van verbanden tussen gegevens met betrekking tot personen en organisaties ten einde zicht te krijgen op de onderlinge relatie hiertussen, zoals het inzichtelijk maken (bijvoorbeeld aan de hand van technisch kenmerk) van de contacten van een target met andere personen en de contacten van die personen met weer andere personen.
Niet-kabelgebonden communicatie	Communicatie die via een draadloze verbinding loopt, namelijk via de ether (bijvoorbeeld satellietverbindingen).
Ontsluiting	Het toegankelijk of doorzoekbaar maken van gegevens.
Ongericht intercepteren	Als niet van tevoren kan worden aangegeven op welke persoon, organisatie of technisch kenmerk de gegevensverwerving gericht is.
Operationeel proces	Het combineren van verworven gegevens met andere (reeds beschikbare) gegevens waarna de gegevens worden geduid en geanalyseerd om rapportages op te stellen die desgewenst aan de verantwoordelijke instanties kunnen worden verstrekt.
Opgeslagen telecommunicatiegegevens	Telecommunicatiegegevens die opgeslagen staan in een geautomatiseerd werk (bijvoorbeeld een computer, een mobiele telefoon of een server).
Persoonsgegevens	Gegevens die betrekking hebben op een identificeerbare of geïdentificeerde, individuele natuurlijke persoon (bijvoorbeeld een naam of een foto).
Ruwe gegevens	Gegevens verkregen door middel van de inzet van bijzondere bevoegdheden die nog *niet* op relevantie zijn beoordeeld.

Searchen	Het verkennen van niet-kabelgebonden communicatie die zijn oorsprong of bestemming in andere landen heeft, met name HF-radioverkeer en satellietcommunicatie.
Sectiehoofd (MIVD)	Functionaris binnen de MIVD die hiërarchisch als volgt is ingebed in de organisatie: directeur, afdelingshoofd, bureauhoofd, *sectiehoofd*.
Signals intelligence (sigint)	Inlichtingen die verzameld worden uit opgevangen elektronische signalen.
Stromende informatie /transport fase	Communicatie die onderweg is van de verzender naar de ontvanger. Deze communicatie bevindt zich in de *transport*-fase. Stromende informatie kan bijvoorbeeld door middel van een tap worden onderschept.
Symbolon	Een project van de AIVD en de MIVD om de inrichting van een gezamenlijke Sigint-Cyber eenheid voor te bereiden. Deze nieuwe eenheid is inmiddels gerealiseerd onder de naam Joint Sigint Cyber Unit.
Teamhoofd (AIVD)	Functionaris binnen de AIVD die hiërarchisch als volgt is ingebed in de organisatie: *hoofd*, directeur, unithoofd, teamhoofd.
Technisch kenmerken	Kenmerken die herleidbaar zijn tot verschillende elementen van telecommunicatie, bijvoorbeeld een telefoonnummer, een IMEI-nummer of een IP-adres.
Telecommunicatie	Communicatie over afstand door middel van elektronische middelen (bijvoorbeeld telefoon, radio, fax en internet).
Telecomprovider	Aanbieder van openbare telecommunicatienetwerken en openbare telecommunicatiediensten (bijvoorbeeld KPN of Vodafone).
Telefonieverkeersgegevens	Telefonieverkeersgegevens zijn verkeersgegevens (zie uitleg onder verkeersgegevens) die zien op telefonie.
Unithoofd (AIVD)	Functionaris binnen de AIVD die hiërarchisch als volgt is ingebed in de organisatie: hoofd, directeur, *unithoofd*, teamhoofd.
Veiligheidsdienst	Een dienst die onderzoek doet naar personen en organisaties die mogelijk een gevaar vormen voor het voortbestaan van de democratische rechtsorde, dan wel voor de veiligheid of voor andere gewichtige belangen van de staat, dan wel voor de veiligheid en de paraatheid van de krijgsmacht.
Veiligheidstaak	Taak gericht op het onderkennen van dreigingen voor het voortbestaan van de democratische rechtsorde (artikel 6, tweede lid, aanhef d Wet op de inlichtingen- en veiligheidsdiensten), dan wel voor de veiligheid of andere gewichtige belangen van de staat, of voor de veiligheid en de paraatheid van de krijgsmacht (artikel 7, tweede lid, aanhef c Wet op de inlichtingen- en veiligheidsdiensten 2002).
Verkeersgegevens	Gegevens betreffende de gebruiker (gebruikersgegevens, bijvoorbeeld naam, adres, woonplaats, nummer), betreffende

	de personen of organisaties met wie de gebruiker verbinding heeft (gehad) of heeft getracht tot stand te brengen ofwel die hebben getracht verbinding met de gebruiker tot stand te brengen (naam, adres, woonplaats, telefoonnummer), gegevens betreffende de verbinding zelf (metagegevens, bijvoorbeeld starttijd, eindtijd, locatiegegevens randapparatuur, nummers randapparatuur) en gegevens betreffende het abonnement (de soort dienst waarvan de gebruiker gebruik maakt of heeft gemaakt, de gegevens van degene die de rekening betaalt) (artikel 28 Wet op de inlichtingen- en veiligheidsdiensten 2002).
Verwervende afdeling	De afdeling binnen de AIVD/MIVD die bij de inzet van bijzondere bevoegdheden betrokken is bij het – al dan niet met technische middelen – verwerven van de gegevens. Dit is een andere afdeling dan de afdeling die het operationele onderzoek uitvoert waarbinnen een bijzondere bevoegdheid wordt ingezet. Bij de AIVD zijn dit de operationele teams, bij de MIVD de operationele bureaus.
VOIP	'Voice over IP', ook wel IP-telefonie. Het betreft bellen via het internetprotocol.
Webforum	Digitale publieke discussiepagina's op het internet. Op sommige forums dienen bezoekers zich aan te melden om toegang te krijgen. Via deze pagina's kunnen de bezoekers veelal ook onderling berichten uitwisselen.
Werkwijze	Het schriftelijke beleid van de diensten en/of de werkwijze die in de praktijk wordt gehanteerd.

Het rapport in vogelvlucht

Naar aanleiding van de onthullingen over de NSA is de Commissie in juli 2013 door de Tweede Kamer gevraagd onderzoek te verrichten naar de activiteiten van de AIVD en de MIVD. Met dit toezichtsrapport beoogt de Commissie tegemoet te komen aan de vragen die in het Parlement en in de media leven over de wijze waarop de Nederlandse diensten verzamelingen (persoons)gegevens op het gebied van telecommunicatie verwerven, gebruiken en met buitenlandse diensten uitwisselen. Deze activiteiten zijn samen te brengen onder de grotere noemer 'gegevensverwerking' en dan met name op het terrein van telecommunicatie, dat wil zeggen alle elektronische vormen van communicatie over afstand: telefoon, fax, radio en internet.

Het algemeen beeld van de Commissie op basis van haar onderzoek is als volgt. De AIVD en de MIVD zijn de afgelopen jaren in toenemende mate gaan werken met verzamelingen (persoons)gegevens. Dit hangt samen met nieuwe technische mogelijkheden en de digitalisering van de samenleving. De Commissie signaleert dat beide diensten zowel bij het verwerven van gegevens als bij de uitwisseling met buitenlandse diensten de bepalingen in de Wiv 2002 als uitgangspunt nemen. Bestaande bevoegdheden worden echter op manieren ingezet die bij de totstandkoming van de wet niet altijd waren voorzien. Naar het oordeel van de Commissie bieden sommige werkwijzen van de diensten op bepaalde vlakken thans onvoldoende waarborgen voor de bescherming van de persoonlijke levenssfeer. In enkele gevallen zijn deze werkwijzen onrechtmatig op basis van de Wiv 2002, bijvoorbeeld vanwege het ontbreken van motivering en/of toestemming op het juiste niveau. De Commissie constateert dat de AIVD en de MIVD in enkele hechte samenwerkingsverbanden verzamelingen (ruwe) gegevens uitwisselen. Hierbij wordt erop vertrouwd dat buitenlandse diensten mensenrechten respecteren en handelen binnen hun eigen wettelijk kader. De Commissie is van mening dat het in het licht van de onthullingen van de afgelopen periode gewenst is om na te gaan of dit vertrouwen nog steeds terecht is. Zij beveelt de betrokken ministers in dit verband tevens aan de samenwerkingsrelaties (ook in internationaal verband) te beoordelen op transparantie en de afwegingen die ten grondslag liggen aan de samenwerking nader te concretiseren.

Het rapport gaat in op de aard van de werkwijzen van de AIVD en de MIVD bij de genoemde vormen van gegevensverwerking. Het betreft een ingewikkelde materie, zowel wat betreft de systemen die aan de orde komen als wat betreft het juridisch toetsingskader. Om de lezer behulpzaam te zijn bij het begrijpen van de bevindingen, bevat het rapport een begrippenlijst waarin op een aantal gebruikte termen een toelichting wordt gegeven. De juridische bijlage bij dit rapport schetst het bredere juridische kader waarbinnen gegevensverwerking behoort plaats te vinden op basis van de Wiv 2002, de Grondwet en het EVRM. Daarnaast bevat het rapport twee geheime bijlagen, één betreffende de AIVD en één betreffende de MIVD. De Commissie toetst in dit rapport of de werkwijzen van de diensten rechtmatig zijn. Concrete gevallen worden beoordeeld in andere toezichtsrapporten van de Commissie, zoals het in april 2014 af te ronden onderzoek inzake de onderzoeksactiviteiten van de AIVD op sociale media.

Aangezien de Commissie zich in haar onderzoek heeft gericht op de verschillende vormen van gegevensverwerking op het gebied van telecommunicatie, is het rapport ook zo opgebouwd, en is aangesloten bij de systematiek en terminologie van de Wiv 2002. Hierbij is de Commissie zich evenwel bewust gebleven van de oorspronkelijke vragen die de Tweede Kamer aan de Commissie heeft gesteld. Aan de hand van deze vragen worden hieronder de belangrijkste bevindingen van dit onderzoek weergegeven.

1. Kan een inschatting worden gegeven van de aard en omvang van wat de Nederlandse inlichtingendiensten doen aan (a) grootschalige dataverzameling (m.n. data fishing), (b) het combineren van data, (c) data opslag en (d) data uitwisseling?

Er zijn verschillende methoden waarmee de AIVD en de MIVD gegevens op het gebied van telecommunicatie verwerven.
Een methode die zonder meer als grootschalig kan worden aangemerkt betreft het ongericht intercepteren van niet-kabelgebonden telecommunicatie (signals intelligence, sigint). Het gaat hierbij om het uit de ether opvangen van vele communicatiesessies en de bijbehorende metagegevens. Na het binnenhalen van deze verzameling gegevens verrichten de diensten metadata-analyse waarbij de metagegevens in kaart worden gebracht en worden gecombineerd met de reeds aanwezige informatie. Daarnaast verkennen de diensten de beschikbare gegevens om te bezien van welke communicatiesessies men de inhoud nader zou willen onderzoeken (search). Na toestemming van de betrokken minister wordt kennis genomen van de inhoud ten behoeve van het operationele proces (selectie). Een andere methode is het binnendringen in geautomatiseerde werken om opgeslagen telecommunicatiegegevens te verwerven (hacken), bijvoorbeeld gegevens uit e-mailaccounts of webfora. Ook worden menselijke bronnen ingezet om gegevens op het gebied van telecommunicatie te verwerven. Andere methodes van gegevensverwerving die in het rapport aan de orde komen, te weten telefoon- en internettaps en het opvragen van telefonieverkeersgegevens en gebruikersgegevens bij telecomproviders, worden door de diensten niet gebruikt voor het grootschalig verwerven van gegevens.

De telecommunicatiegegevens die de diensten met gebruik van deze methoden verwerven, zowel de inhoud van de communicatie als de metagegevens, zijn bedoeld om te benutten in het inlichtingenproces. De diensten combineren de gegevens met andere gegevens en na duiding en analyse stellen de diensten rapportages op die desgewenst aan de verantwoordelijke instanties kunnen worden verstrekt.
Hiertoe worden de gegevens na verkrijging eerst digitaal opgeslagen op servers en ontsloten via computerprogramma's (applicaties). In de verworven, dan nog ruwe gegevens zoeken de diensten naar relevante informatie, die vervolgens wordt bewerkt en geanalyseerd (geëvalueerde gegevens). De resterende gegevens blijven in de meeste gevallen enige tijd bewaard. De diensten gebruiken diverse analyseapplicaties waarmee gegevens worden samengevoegd en geanalyseerd. In de meeste gevallen is de toegang tot ruwe gegevens binnen de organisatie beperkt tot medewerkers die zijn betrokken bij het onderzoek in het kader waarvan de gegevens zijn verworven. Uitzonderingen hierop zijn de applicaties waarvan de AIVD gebruik maakt bij metadata-analyse en de applicatie die de AIVD gebruikt voor de ontsluiting van webfora. Deze applicaties zijn breder toegankelijk.

De samenwerking van de AIVD en de MIVD met buitenlandse diensten kan bestaan uit het verstrekken en ontvangen van (persoons)gegevens en uit het verlenen van ondersteuning zoals het inzetten van een bijzondere bevoegdheid op verzoek van een partnerdienst. Binnen hechte samenwerkingsrelaties kan het voorkomen dat hierover structurele afspraken worden gemaakt. Dit gebeurt ten aanzien van onderwerpen waar een gezamenlijke aanpak noodzakelijk wordt geacht, zoals in het kader van de strijd tegen het terrorisme en van militaire operaties in het buitenland. Binnen bepaalde hechte samenwerkingsrelaties van de AIVD en de MIVD met buitenlandse diensten worden verzamelingen (ruwe) gegevens uitgewisseld, al dan niet op structurele basis.

2. Welke ruimte laat de Wet op de inlichtingen- en veiligheidsdiensten 2002 (Wiv) voor onder de eerste onderzoeksvraag genoemde vier afzonderlijke activiteiten? Kan worden aangegeven of en waar de activiteiten niet of deels rechtmatig plaatsvinden binnen de Wiv? Wat is specifiek de relatie tussen de artikelen 24-27 en 59 van de Wiv?

De Commissie constateert dat de methoden die de AIVD en de MIVD aanwenden om gegevens op het gebied van telecommunicatie te verzamelen passen binnen de bevoegdheden die in de Wiv 2002 aan de diensten zijn toegekend. Er is geen sprake van het stelselmatig buiten de wet om verwerven van verzamelingen van (persoons)gegevens door de AIVD en de MIVD.

Wel constateert de Commissie dat technologische ontwikkelingen het vandaag de dag mogelijk maken om bestaande bevoegdheden op nieuwe, niet altijd door de wetgever voorziene, manieren in te zetten. Hiermee hangt samen dat door de digitalisering van de samenleving en de daarmee verband houdende sterke intensivering van het communicatieverkeer veel meer gegevens op het gebied van telecommunicatie beschikbaar zijn. De potentiële inbreuk die de diensten met deze methoden kunnen maken op de persoonlijke levenssfeer gaat dan ook veel verder dan in 2002 mogelijk was. Dit heeft tot gevolg dat op een aantal vlakken de werkwijzen van de diensten thans onvoldoende waarborgen bieden voor de bescherming van de persoonlijke levenssfeer, terwijl hierbij strikt genomen de Wiv 2002 niet wordt overschreden.

Zo wordt bij de analyse van metadata na ongerichte interceptie niet gemotiveerd waarom dit voldoet aan het noodzakelijkheids-, proportionaliteits- en subsidiariteitsvereiste, noch is dit proces anderszins met waarborgen omkleed. De Commissie beveelt aan een regeling voor de verwerking van metagegevens op te nemen in de Wiv 2002. Daarnaast signaleert de Commissie dat bij het gebruiken en bewaren van webfora die in hun geheel door de AIVD zijn verworven meer aandacht moet worden besteed aan het waarborgen van de persoonlijke levenssfeer.

De Commissie is daarnaast werkwijzen tegengekomen die zij op basis van de Wiv 2002 als onrechtmatig kwalificeert. Zo schieten de diensten bij de inzet van menselijke bronnen in bepaalde situaties tekort in het vooraf motiveren van de specifieke activiteiten en het niet op het juiste niveau toestemming vragen voor de verrichte activiteiten. Bij de inzet van de hackbevoegdheid wordt intern in bepaalde situaties niet op het juiste niveau toestemming gevraagd. Daarnaast is, zoals de Commissie in haar eerdere rapporten al constateerde, de praktijk van het searchen na de interceptie van sigint deels in strijd met de Wiv 2002 en wordt de selectie van sigint zelf onvoldoende gemotiveerd.

De Wiv 2002 geeft de AIVD en de MIVD een ruime bevoegdheid om samen te werken met buitenlandse diensten. Bij de totstandkoming van de Wiv 2002 is niet expliciet overwogen hoe omgegaan moet worden met de uitwisseling van verzamelingen (ruwe) persoonsgegevens. De Commissie constateert dat de AIVD en de MIVD op basis van de Wiv 2002 tot deze uitwisseling kunnen overgaan en dit in de praktijk in verschillende samenwerkingsverbanden ook doen. Het verstrekken van verzamelingen gegevens, zowel metagegevens als inhoudelijke communicatie, in de onderzochte samenwerkingsverbanden beoordeelt de Commissie als rechtmatig. Daarnaast mogen de AIVD en de MIVD op verzoek van buitenlandse diensten ondersteuning leveren, waaronder ook de inzet van bevoegdheden zoals die zijn beschreven in de artikelen 24-27 Wiv 2002. Daarbij moet wel voldaan zijn aan de in de wet gestelde eisen voor de inzet van deze bijzondere bevoegdheden. In de onderzochte samenwerkingsverbanden op het terrein van de

uitwisseling van verzamelingen gegevens is de Commissie op één onrechtmatige werkwijze gestuit. Zij constateert dat de MIVD ten behoeve van buitenlandse diensten de selectiebevoegdheid inzet zonder hiervoor toestemming van de minister te verkrijgen, hetgeen onrechtmatig is.

3. Hoe verhouden de onder de eerste onderzoeksvraag genoemde vier afzonderlijke activiteiten zich tot de Nederlandse grondwet en het Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden (EVRM)?

In de Wiv 2002 hebben de waarborgen die door artikel 8 van het EVRM, de jurisprudentie van het EHRM en de artikelen 10 en 13 van de Grondwet worden geboden hun weerslag gekregen. Het uitgangspunt hierbij is geweest dat het verwerken van persoonsgegevens door de diensten in meer of mindere mate inbreuk maakt op de persoonlijke levenssfeer van de betrokkenen en dat de mate van inbreuk in balans dient te zijn met het doel ervan, te weten het beschermen van de nationale veiligheid. Om te bewerkstelligen dat deze balans inderdaad steeds aanwezig is, heeft de wetgever een aantal structurele waarborgen opgenomen in de Wiv 2002 zoals een limitatieve opsomming van de taken van de diensten en de bijbehorende inlichtingenmiddelen, de vereisten van noodzakelijkheid, proportionaliteit en subsidiariteit waaraan voldaan dient te zijn bij de inzet van een bijzondere bevoegdheid en het toestemmingsvereiste voor deze inzet, intern of op het niveau van de minister en de algemene vereisten die gelden voor de verwerking van (persoons)gegevens waaronder de vereisten van noodzakelijkheid, behoorlijkheid en zorgvuldigheid.

Bij het toetsen van de werkwijzen van de AIVD en de MIVD aan de Wiv 2002, zoals weergegeven bij de beantwoording van vraag 2, neemt de Commissie deze waarborgen uit het EVRM en de Grondwet ook mee.

4. Hoe is de toetsing op proportionaliteit en subsidiariteit – zoals gevraagd in het EVRM – geregeld wanneer via buitenlandse diensten informatie over Nederlandse burgers wordt verkregen?

(Persoons)gegevens met betrekking tot Nederlandse burgers kunnen door de AIVD en de MIVD worden verkregen doordat een buitenlandse dienst de gegevens verstrekt of doordat een buitenlandse dienst ondersteuning levert, bijvoorbeeld door de inzet van een bijzondere bevoegdheid ten behoeve van de AIVD of de MIVD. Het verstrekken van gegevens of het verlenen van ondersteuning door buitenlandse diensten vindt vrijwel altijd plaats op basis van een verzoek van de AIVD of de MIVD. De toetsing of de gegevensverstrekking of de ondersteuning voldoet aan de vereisten van noodzakelijkheid, proportionaliteit en subsidiariteit dient te worden gemaakt door de buitenlandse dienst die de gegevens verstrekt of de ondersteuning levert. De AIVD en de MIVD spelen hierin als ontvanger van de gegevens of de ondersteuning een beperktere rol. De AIVD en de MIVD dienen wel voorafgaande aan het indienen van een verzoek om bepaalde gegevens of ondersteuning een afweging te maken in hoeverre de gewenste gegevensverstrekking of ondersteuning voldoet aan de vereisten van noodzakelijkheid, proportionaliteit en subsidiariteit. Het is de AIVD en de MIVD niet toegestaan een buitenlandse dienst te verzoeken een bevoegdheid in te zetten waar de Nederlandse diensten zelf niet over beschikken (de U-bochtconstructie). De diensten moeten zich verder onthouden van het gebruik van gegevens van buitenlandse diensten als er concrete aanwijzingen zijn dat de gegevens zijn verworven op een manier die naar Nederlandse maatstaven een ongeoorloofde inbreuk op de persoonlijke levenssfeer of op een ander grond- of mensenrecht oplevert. Tot slot zij opgemerkt dat er geen aparte toets is ten

aanzien van Nederlandse burgers, aangezien de Wiv 2002, de Grondwet en het EVRM geen onderscheid maken naar nationaliteit.

Met het bovenstaande heeft de Commissie naar aanleiding van de aan haar door de Tweede Kamer gestelde vragen de hoofdlijnen van haar bevindingen geschetst. De Commissie beseft evenwel dat met deze conclusies nog niet een duidelijk antwoord is gegeven op een aantal belangrijke vragen die in de samenleving worden gesteld over de activiteiten van de Nederlandse diensten. Daarom zal zij in de volgende alinea's kort op een aantal van deze vragen ingaan.

De vraag of de AIVD en de MIVD grootschalig en ongericht gegevens verwerven op het gebied van telecommunicatie kan in twee delen worden beantwoord. Ten aanzien van niet-kabelgebonden communicatie is het antwoord op die vraag 'ja'. De wet staat dat de diensten ook toe (artikel 27 lid 1 Wiv 2002) en voorziet in de nodige waarborgen voor het verwerken van de aldus ongericht geïntercepteerde gegevens (artikel 27, leden 3-10 Wiv 2002). Ten aanzien van kabelgebonden communicatie is het antwoord 'nee', waar het gaat om stromende communicatie, dat wil zeggen communicatie die onderweg is van verzender naar ontvanger. Hiertoe zijn de diensten op basis van de Wiv 2002 niet bevoegd. De Commissie heeft vastgesteld dat er geen ongerichte interceptie van kabelgebonden telecommunicatie plaatsvindt door de AIVD en de MIVD. Wat wel gebeurt, is dat opgeslagen, dus niet stromende, telecommunicatiegegevens worden verworven door met name de inzet van menselijke bronnen of door de inzet van de hackbevoegdheid en dat het daarbij kan gaan om verzamelingen (persoons)gegevens. De Commissie hanteert de term 'ongericht' als niet van tevoren kan worden aangegeven op welke persoon, organisatie of technisch kenmerk de gegevensverwerving gericht is. In bepaalde gevallen zou de verwerving van verzamelingen (persoons)gegevens door menselijke bronnen op grond van deze definitie als ongericht kunnen worden aangemerkt. De Commissie benadrukt dat dit niet betekent dat er vanuit de taakstelling van de diensten geen aanleiding is de gegevens te verwerven. Zij heeft geen aanwijzingen dat de diensten bij de verwerving van telecommunicatiegegevens door menselijke bronnen hun wettelijke taken te buiten gaan.

Het antwoord op de vraag of de AIVD en de MIVD in het kader van de samenwerking met buitenlandse diensten gebruik hebben gemaakt van telecommunicatiegegevens die in strijd met de Nederlandse wet zijn verzameld is niet met een eenvoudig 'ja' of 'nee' te beantwoorden. Buitenlandse diensten waarmee de AIVD en de MIVD samenwerken kunnen beschikken over meer of andere bevoegdheden dan de Nederlandse diensten. Het ontvangen van gegevens wordt pas onrechtmatig als het bij de Nederlandse diensten bekend is of bekend verondersteld mag worden dat deze gegevens door de buitenlandse dienst zijn verzameld op een manier die een ongeoorloofde inbreuk op de persoonlijke levenssfeer (of een ander grondrecht) oplevert. Dat zou onacceptabel zijn, omdat dan afbreuk wordt gedaan aan de bescherming van grondrechten waartoe de Nederlandse staat zich via internationale verdragen heeft verplicht. Het is echter in de samenwerking tussen inlichtingen- en veiligheidsdiensten, ook in hechte samenwerkingsrelaties, niet gebruikelijk om te delen hoe gegevens zijn verzameld. In de onderzochte hechte samenwerkingsverbanden vertrouwen de AIVD en de MIVD er in het algemeen op dat de buitenlandse diensten mensenrechten respecteren en handelen binnen de eigen nationale regelgeving totdat er aanwijzingen zijn voor het tegendeel. De onthullingen van de afgelopen periode kunnen aangemerkt worden als dergelijke aanwijzingen en maken dat het gewenst is na te gaan of dit vertrouwen nog steeds terecht is. Zij beveelt de betrokken ministers in dit verband tevens aan de samenwerkingsrelaties (ook op internationaal niveau) te beoordelen op transparantie en de afwegingen die ten grondslag liggen aan de samenwerking nader te concretiseren.

De Commissie heeft in haar onderzoek geen aanwijzingen gevonden dat de AIVD en de MIVD buitenlandse diensten, bij wijze van U-bochtconstructie, verzoeken gegevens te verzamelen op een manier die henzelf niet is toegestaan. Wel is de Commissie gestuit op de situatie dat sommige buitenlandse diensten waarmee de Nederlandse diensten samenwerken de bevoegdheid hebben om ongericht kabelgebonden communicatie te intercepteren. Dit valt voor hen ook onder het begrip sigint. De Nederlandse diensten beschikken niet over deze bevoegdheid. De Commissie constateert dat wanneer de AIVD en de MIVD sigint van die buitenlandse diensten ontvangen, hetgeen met enige regelmaat voorkomt, zij daardoor wellicht ook gegevens ontvangen die het resultaat zijn van kabelgebonden interceptie. De Commissie stelt zich op het standpunt dat het ongericht intercepteren van kabelgebonden telecommunicatie niet op zichzelf reeds een ongeoorloofde inbreuk op de persoonlijke levenssfeer of op een ander grond- of mensenrecht oplevert. Aan de AIVD en de MIVD is immers in de Wiv 2002 een vergelijkbare bevoegdheid toegekend ten aanzien van niet-kabelgebonden telecommunicatie. Bij de totstandkoming van de Wiv 2002 is geen expliciete grondrechtelijke afweging gemaakt over het verschil tussen kabelgebonden en niet-kabelgebonden telecommunicatie. Ook kan niet op voorhand worden gezegd dat kabelgebonden interceptie, indien voorzien van voldoende waarborgen, op zichzelf in strijd is met het EVRM of andere mensenrechtenverdragen. De Commissie acht het in dit verband toegestaan dat de AIVD en de MIVD samenwerken met deze buitenlandse diensten, ook als niet uitgesloten kan worden dat zij gegevens ontvangen die zijn verkregen door ongerichte interceptie van kabelgebonden telecommunicatie.

Ook wordt regelmatig de vraag gesteld of de AIVD en de MIVD op enigerlei wijze medewerking hebben verleend aan het verzamelen van telecommunicatiegegevens in strijd met de Nederlandse wet. Het zou hierbij gaan om het toestaan dat buitenlandse diensten in Nederland telefoon- en/of internetverkeer tappen. De Wiv 2002 staat het buitenlandse diensten alleen toe activiteiten te ontplooien op Nederlands grondgebied indien hiervoor door de verantwoordelijke minister toestemming is gegeven en indien dit geschiedt onder supervisie en verantwoordelijkheid van de AIVD of de MIVD. De Commissie heeft daarbij geen aanwijzingen gevonden dat buitenlandse diensten met medewerking van de AIVD of de MIVD zelfstandige toegang hebben verkregen tot Nederlandse telefoon- of internetverbindingen.

Tot slot merkt de Commissie op dat op een aantal thema's die in dit toezichtsrapport aan de orde komen (structureel) onderzoek wordt verricht door de Commissie dan wel dat een dergelijk onderzoek zal worden ingesteld. In deze onderzoeken worden naast de werkwijze ook concrete gevallen getoetst. De Commissie verwijst naar haar lopende diepte- en vervolgonderzoeken naar de inzet van de afluisterbevoegdheid en van de bevoegdheid tot de selectie van sigint door de AIVD (verwachte afronding periode september 2012 t/m augustus 2013: begin april 2014), het onderzoek door de AIVD op sociale media (verwachte afronding: begin april 2014), de samenwerking met buitenlandse diensten door de MIVD (verwachte afronding: mei 2014) en de samenwerking met buitenlandse diensten door de AIVD (verwachte afronding: augustus 2014). In het eerste kwartaal van 2014 zal tevens een (doorlopend) vervolgonderzoek worden ingesteld naar de inzet van het middel sigint door de MIVD.

1 Inleiding

Vanaf juni 2013 zijn druppelsgewijs de onthullingen over de praktijken van de Amerikaanse National Security Agency (NSA) in de wereldpers verschenen op basis van informatie gelekt door de voormalige werknemer van die dienst Edward Snowden. Als eerste kwam het surveillanceprogramma PRISM onder de aandacht te staan. Dit programma zou volgens de gelekte documenten en interviews met Snowden gericht zijn op het binnenhalen dan wel doorzoeken van de chatgesprekken, e-mails, foto's en video's die zijn opgeslagen op de servers van grote internetbedrijven als Microsoft, Yahoo, Google, Facebook, Skype en YouTube.

In de Nederlandse media zijn in de loop van juni verscheidene vragen opgeworpen over de betrokkenheid van de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) en de Militaire Inlichtingen- en Veiligheidsdienst (MIVD) (hierna ook wel: de diensten) bij, samengevat, het inwinnen en uitwisselen met de VS van bulkdata betreffende internetverkeer en telecommunicatie. Dit heeft geleid tot Kamervragen begin juni over met name de projecten Symbolon en Argo II en het mogelijk door de AIVD en de MIVD aftappen van het internetknooppunt Amsterdam Internet Exchange (AMS-IX).[1] Op 21 juni 2013 heeft de minister van Binnenlandse Zaken en Koninkrijksrelaties (BZK) aan de Tweede Kamer een brief geschreven waarin uiteen is gezet hoe de wettelijke bevoegdheden van de Nederlandse inlichtingen- en veiligheidsdiensten zich verhouden tot het PRISM-programma of vergelijkbare methoden van informatievergaring.[2] De minister stelde in de brief dat de AIVD en de MIVD het computerprogramma PRISM niet gebruiken. Voorts lichtte hij toe dat de diensten geen onbelemmerde, onbeperkte toegang hebben tot het internetverkeer en het mobiele telefoonverkeer, ook niet via buitenlandse inlichtingen- en/of veiligheidsdiensten (hierna: buitenlandse diensten). Op het gebied van samenwerking met buitenlandse diensten legde de minister uit dat het de AIVD en de MIVD niet is toegestaan andere landen verzoeken te doen die op grond van de Wet op de inlichtingen- en veiligheidsdiensten 2002 (Wiv 2002) niet zijn toegestaan met de kanttekening dat bij internationale samenwerking tussen diensten doorgaans niet wordt gedeeld hoe gegevens zijn verkregen.

Op 26 juni 2013 heeft de Tweede Kamer een hoorzitting gehouden met deskundigen over het verzamelen en bewaren van persoonsgegevens door Nederlandse en buitenlandse diensten. Op dezelfde dag is ook een besloten hoorzitting gehouden met medewerkers van de diensten.

Een week later, op 4 juli, was aanvankelijk een Algemeen Overleg (AO) geagendeerd naar aanleiding van de berichtgeving over PRISM. Het AO werd uiteindelijk geannuleerd en in de procedurevergadering op 4 juli werd besloten de Commissie van Toezicht betreffende de Inlichtingen- en Veiligheidsdiensten (verder te noemen: de Commissie) voluit op grond van artikel 78, tweede lid, Wiv 2002 te verzoeken een onderzoek in te stellen naar de dataverzameling door de AIVD en de MIVD met daarbij een aantal onderzoeksvragen.[3] De Commissie heeft dit verzoek op 23 juli 2013 ontvangen. De volgende onderzoeksvragen zijn aan de Commissie voorgelegd:

[1] *Aanhangsel Handelingen II* 2012/13, nr. 2649.
[2] *Kamerstukken II* 2012/13, 30 977, nr. 56.
[3] *Kamerstukken II* 2012/13, 30 977, nr. 57.

1. Kan een inschatting worden gegeven van de aard en omvang van wat de Nederlandse inlichtingendiensten doen aan (a) grootschalige dataverzameling (m.n. data fishing), (b) het combineren van data, (c) data opslag en (d) data uitwisseling?

2. Welke ruimte laat de Wet op de inlichtingen- en veiligheidsdiensten 2002 (Wiv) voor onder de eerste onderzoeksvraag genoemde vier afzonderlijke activiteiten? Kan worden aangegeven of en waar de activiteiten niet of deels rechtmatig plaatsvinden binnen de Wiv? Wat is specifiek de relatie tussen de artikelen 24-27 en 59 van de Wiv?

3. Hoe verhouden de onder de eerste onderzoeksvraag genoemde vier afzonderlijke activiteiten zich tot de Nederlandse grondwet en het Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden (EVRM)?

4. Hoe is de toetsing op proportionaliteit en subsidiariteit – zoals gevraagd in het EVRM – geregeld wanneer via buitenlandse diensten informatie over Nederlandse burgers wordt verkregen?

De Commissie heeft zich naar aanleiding van dit verzoek beraden op de vraag hoe een onderzoek door haar ingericht dient te worden teneinde in een aanvaardbaar tijdsbestek zo goed mogelijk antwoord te geven op de (maatschappelijke) vragen die zijn gerezen. Zij heeft besloten het onderzoek te richten op gegevensverwerking door de AIVD en de MIVD, omdat het begrip gegevensverwerking op grond van de Wiv 2002 elke handeling of elk geheel van handelingen met betrekking tot gegevens omvat. Het omvat derhalve mede het verzamelen, vastleggen, bewaren, samenbrengen en verstrekken van gegevens (artikel 1 sub f Wiv 2002). Zij heeft besloten daarbij de focus te leggen op gegevensverwerking op het gebied van telecommunicatie. De term 'telecommunicatie' betekent letterlijk het overbrengen van informatie over afstand en omvat, naast oude methodes als telegrafie en vlaggensignalen die uiteraard niet relevant zijn voor dit onderzoek, alle elektronische vormen van communicatie over afstand: telefoon, fax, radio, internet.

Binnen dit algemene veld van gegevensverwerking op het gebied van telecommunicatie door de AIVD en de MIVD heeft de Commissie, in lijn met het verzoek van de Tweede Kamer, een viertal onderwerpen gekozen die in ieder geval aan de orde zullen komen:

1. De reikwijdte van de algemene en bijzondere bevoegdheden van de diensten tot gegevensverwerking op het gebied van telecommunicatie, mede in relatie tot de Grondwet en het EVRM.

2. De wijze waarop gebruik wordt gemaakt van verschillende soorten gegevensbestanden door de diensten en de regels die gelden voor dat gebruik.

3. De mogelijkheden en beperkingen van de uitwisseling van gegevens met buitenlandse inlichtingen- en/of veiligheidsdiensten.

4. De wijze waarop de door het EVRM gestelde toetsingsnormen – noodzakelijkheid, proportionaliteit en subsidiariteit – een rol spelen bij de gegevensverwerking door de diensten, in het bijzonder bij de gegevensuitwisseling met buitenlandse inlichtingen- en/of veiligheidsdiensten.

De Commissie heeft haar onderzoek op 5 augustus 2013 aangekondigd aan de ministers van BZK en Defensie en aan de voorzitters van beide Kamers der Staten-Generaal.

In de periode na de aankondiging van het onderzoek hield de stroom van berichtgeving in de media over de activiteiten van de NSA aan, vanaf augustus 2013 onder meer over het door de NSA afluisteren van diverse buitenlandse dan wel internationale instellingen en functionarissen.[4] Op 13 september verscheen de kabinetsbrede reactie op de onthullingen in de media, waarin het kabinet onder meer verwijst naar het onderzoek dat door de Commissie wordt uitgevoerd en naar diverse overleggen in EU-verband met de Amerikaanse overheid met het doel wederzijds inzicht te verkrijgen in elkaars inlichtingenprogramma's, de wettelijke basis daarvoor en het toezicht daarop.[5]

Op 16 oktober werd in een AO met de minister van BZK over de kabinetsbrede reactie gesproken. Het centrale discussiepunt in dit AO was of er in Europees verband gereageerd moet worden op de berichten over spionage door de Verenigde Staten of juist vanuit Nederland, in bilateraal verband. Aansluiten bij het Duitse initiatief voor een anti-spionageakkoord werd genoemd als optie voor een reactie vanuit Nederland. Op dit punt deed de minister de toezegging een bilaterale oplossing te verkennen na uitkomst van het feitenonderzoek door de VS-EU-expertgroep, ingesteld op initiatief van de Europese Commissie. In het AO werd ook aandacht besteed aan het begrip metadata-analyse. De minister heeft toegelicht dat metadata-analyse in essentie inhoudt dat de telefoonnummers van gekende terroristen worden vergeleken met de bulk aan metagegevens om te bezien welke informatie dit oplevert. Het kan zijn dat een persoon die nog niet onder de aandacht van de dienst staat in dezelfde cirkel opduikt als de gekende terroristen. De minister heeft verder uitgelegd dat dit in Nederland alleen is toegestaan ten aanzien van niet-kabelgebonden communicatie, welke bijna altijd betrekking heeft op buitenlandse contacten. Hij voegde daaraan toe dat de Commissie-Dessens zich beraadt op de vraag in hoeverre deze techniekafhankelijke benadering dient te worden voortgezet.[6]

Het debat in Nederland nam op 21 oktober een nieuwe wending met het bericht op de website Tweakers.net dat de NSA alleen al in december 2012 de metagegevens van 1,8 miljoen Nederlandse telefoongesprekken zou hebben verzameld. Dit bericht leidde na een verzoek op initiatief van D66 tot een schriftelijke reactie van de minister van BZK op 28 oktober.[7] In deze reactie gaf de minister aan dat het kabinet zich, gezien de Amerikaanse wetgeving – waaronder de Foreign Intelligence Surveillance Act (FISA) – bewust is van de mogelijkheid dat de NSA telefooncommunicatie kan onderscheppen. Aangegeven werd dat het kabinet het intercepteren en het analyseren van metagegevens op zichzelf een aanvaardbare methode acht in het kader van onderzoek naar terroristen en andere gevaren voor de nationale veiligheid of in het kader van militaire operaties. Wanneer andere landen menen dat er een goede reden is om in of vanuit Nederland inlichtingen te verzamelen, dient er echter eerst een verzoek te worden voorgelegd aan de AIVD of de MIVD zodat beoordeeld kan worden of het voorgenomen optreden binnen de kaders van de Nederlandse wet valt, aldus de minister in zijn reactie. De minister deelde voorts mede dat de Nederlandse inlichtingen- en veiligheidsdiensten in gesprek zijn met de NSA om te komen tot een bilaterale oplossing. Hij gaf aan dat Nederland het initiatief van Duitsland en

[4] 'VS luisteren Verenigde Naties af', *ANP* 25 augustus 2013; 'NSA bespioneert Frans ministerie', *ANP* 1 september 2013; 'Brazilië woedend op VS over spionage', *Volkskrant* 13 september 2013; 'NSA bespioneerde ambassade India', *ANP* 25 september 2013, ANP; 'Duitse kritiek op digitale bezettingsmacht', *NRC Handelsblad* 30 oktober 2013; 'NSA luisterde ook Paus af', 30 oktober 2013, www.nos.nl; 'NSA hield ook Ban Ki-Moon in de gaten', 2 november 2013, www.nu.nl.
[5] *Kamerstukken II* 2012/13, 30 977, nr. 61.
[6] *Kamerstukken II* 2012/13, 30 977, nr. 71.
[7] *Kamerstukken II* 2012/13, 30 977, nr. 63.

Frankrijk [Commissie: om te komen tot een anti-spionageakkoord met de VS] positief beoordeelt en waar mogelijk een actieve bijdrage zal leveren.

In een uitzending van het programma Nieuwsuur op 30 oktober liet de minister van BZK weten een bericht te hebben ontvangen van de NSA waarin werd aangegeven dat van de miljoenen afgeluisterde gesprekken in Europa, waarover in de media werd gesproken, inderdaad de metagegevens zijn verzameld. Daarmee werd volgens de minister impliciet bevestigd dat de genoemde aantallen – 1,8 miljoen in december 2012 wat Nederland betreft – juist zijn. De minister gaf in het programma aan dat de AIVD deze gegevens in ieder geval niet heeft verschaft aan de NSA. Daarnaast merkte hij op het niet acceptabel te vinden dat men schouder aan schouder het terrorisme bestrijdt en ondertussen elkaar afluistert.

In de media bleven kritische vragen gesteld worden over de rol van de AIVD in de activiteiten van de NSA ten aanzien van Nederland. Op 30 en 31 oktober verschenen diverse berichten waarin, kort samengevat, werd gesteld dat de AIVD op enigerlei wijze meewerkt aan het door de NSA verzamelen van Nederlandse metagegevens.[8] Aanleiding voor deze berichten was een screenshot van een document betreffende de samenwerking van de NSA met verschillende buitenlandse diensten gepubliceerd door de Spaanse krant *El Mundo*.

Het kabinet reageerde op 31 oktober schriftelijk op twee ingediende moties[9] inzake de acties die het kabinet onderneemt naar aanleiding van de berichtgeving over de NSA.[10] In de brief aan de Tweede Kamer deelde het kabinet mede dat Nederland zowel in gesprek met de NSA zoekt naar een bilaterale oplossing, als waar mogelijk een positieve bijdrage zal leveren aan het Frans-Duitse initiatief van een anti-spionageakkoord met de Verenigde Staten. In reactie op het verzoek om opheldering te vragen over wie afgeluisterd wordt en het inzicht daarover te delen met de Tweede Kamer gaf het kabinet aan hierover in gesprek te zijn met de Verenigde Staten en – waar nodig vertrouwelijk – de Tweede Kamer te zullen informeren over de uitkomst.

De internationale samenwerkingverbanden tussen inlichtingen- en veiligheidsdiensten kwamen verder in de belangstelling naar aanleiding van een artikel dat *The Guardian* op 1 november 2013 publiceerde over de samenwerking tussen het Britse Government Communications Headquarters (GCHQ) en diverse Europese inlichtingen- en veiligheidsdiensten.[11] In dit artikel werd gesteld dat, naast GCHQ zelf, ook de Duitse, Franse, Spaanse en Zweedse diensten methodes hebben ontwikkeld om massaal internet- en telefoonverkeer te monitoren. Over de Nederlandse diensten werd gesteld dat GCHQ de AIVD en de MIVD in 2008 heeft geadviseerd over juridische knelpunten waar zij tegenaan liepen bij het verwerken van internetverkeer.

In een artikel in de Volkskrant op 4 november is onder meer geschreven over de samenwerking van de NSA met buitenlandse diensten in het zogenaamde *five eyes* samenwerkingsverband, waarin de diensten van vijf Angelsaksische landen zouden

---

[8] 'AIVD werkte mogelijk mee aan het onderscheppen metagegevens 1,8 miljoen telefoontjes', 30 oktober 2013, www.tweakers.net; 'AIVD werkt samen met NSA', *NRC Handelsblad* 30 oktober 2013, www.nrc.nl; 'AIVD hielp mogelijk NSA bij aftappen 1,8 miljoen telefoontjes', *Volkskrant* 30 oktober 2013; 'AIVD staat aftappen NSA toe', *Algemeen Dagblad* 31 oktober 2013.

[9] *Kamerstukken II* 2013/14, 21 501-20, nr. 812 en nr. 813.

[10] *Kamerstukken II* 2013/14, 30 977, nr. 64.

[11] 'GCHQ and European spy agencies worked together on mass surveillance', *The Guardian* 1 november 2013.

participeren, en het bredere *nine eyes* samenwerkingsverband waaraan naast de Angelsaksische landen ook Frankrijk, Nederland, Denemarken en Noorwegen zouden deelnemen. Er zouden ook een *14 eyes* samenwerkingsverband bestaan en een samenwerkingsverband van NAVO-lidstaten. Dit artikel leidde tot een verzoek van de Tweede Kamer aan de minister van BZK om een reactie. De minister gaf in zijn reactie van 5 november aan dat de AIVD en de MIVD binnen de kaders van de wet samenwerken met buitenlandse diensten. De minister herhaalde tevens wat hij ook al aangaf in zijn brief van 21 juni aan de Tweede Kamer; dat de AIVD en de MIVD geen verzoeken mogen doen aan buitenlandse diensten die op grond van de Nederlandse wet niet zijn toegestaan.[12] Gemeld werd voorts dat in het openbaar geen mededelingen kunnen worden gedaan over specifieke samenwerkingsrelaties of operaties van de AIVD en de MIVD.[13]

Op 6 november werd wederom een AO gehouden met de minister van BZK over met name de berichten betreffende de NSA. Het Kamerlid Van Raak (SP) stelde er niet meer van overtuigd te zijn dat de AIVD en de MIVD louter toeschouwers zijn. Hiervoor droeg hij drie redenen aan: (1) de geheime aanbesteding voor het programma genaamd Argo II, dat volgens hem bedoeld is om informatie te analyseren die alleen maar verzameld kan zijn op de manier waarop de Amerikanen en de Engelsen dat doen; (2) hij heeft de indruk dat de AIVD en de MIVD informatie hebben gekregen van de Amerikanen en de Engelsen die de vraag moet hebben opgeroepen: hoe kunnen zij aan dit soort informatie komen? (3) het bericht dat Nederland behoort tot het *nine eyes* samenwerkingsverband. De twijfels die de Socialistische Partij (SP) stelt te hebben bij de rol van de AIVD en de MIVD werden in grote lijnen gedeeld door GroenLinks (GL), Democraten 66 (D66) en het Christen Democratisch Appèl (CDA); ook deze partijen wilden weten of de Nederlandse diensten op enigerlei wijze medewerking hebben verleend aan het door de NSA verwerven van Nederlandse metagegevens. Op het onderwerp metagegevens lichtte de minister toe dat het technisch alleen mogelijk is om metagegevens te verzamelen als er sprake is van fysieke toegang tot de telefooncentrale. Indien de Verenigde Staten beschikken over de metagegevens van 1,8 miljoen Nederlandse gesprekken, moet het derhalve gaan om gesprekken tussen Nederland en de Verenigde Staten of tussen Nederland en een ander land.[14]

In het AO van de vaste Kamercommissie voor BZK van 6 november 2013 is tevens het onderhavige onderzoek van de Commissie ter sprake gekomen. Het Kamerlid Schouw (D66) stelde een opmerkelijk verschil te constateren tussen het verzoek aan de Commissie vanuit de Tweede Kamer en het onderzoek dat de Commissie heeft aangekondigd. Het ging hem daarbij om het gebruik door de Commissie van het woord 'gegevensverwerking' in plaats van 'verzamelen van gegevens' en om het gebruik van het woord 'mogelijkheden' in plaats van 'feiten', waar wordt gesproken over de samenwerking met buitenlandse diensten. Aan het einde van het AO is besloten dat de minister deze punten onder de aandacht van de Commissie zou brengen. Dit is in eerste instantie telefonisch gebeurd en later ook in een brief van het hoofd van de AIVD. De Commissie heeft in het telefoongesprek met de griffier van de vaste Kamercommissie voor BZK naar aanleiding van het AO laten weten dat gegevensverwerking op grond van artikel 1 Wiv 2002 een breed begrip is waar ook gegevensverzameling onder valt en voorts dat zij ook onderzoek doet naar de werkwijze van de AIVD en de MIVD bij de uitwisseling van gegevens op het gebied van telecommunicatie met buitenlandse diensten.

---

[12] *Kamerstukken II* 2012/13, 30 977, nr. 56.
[13] *Kamerstukken II* 2012/13, 30 977, nr. 65.
[14] *Kamerstukken II* 2013/14, 30 977, nr. 75.

Op 6 november werd tevens bekend dat een coalitie van journalisten, advocaten en belangenorganisaties een rechtszaak heeft aangespannen tegen de minister van BZK om te bewerkstelligen dat de AIVD stopt met het gebruiken van door de NSA in strijd met de Nederlandse wet verkregen gegevens.[15]

Op 30 november publiceerde het NRC Handelsblad een artikel op basis van een gelekt document van de NSA, waaruit zou blijken dat de AIVD en de MIVD webfora hacken. In het artikel worden enkele deskundigen geciteerd, die vraagtekens zetten bij de rechtmatigheid van dergelijke hacks.[16] De AIVD publiceerde dezelfde dag een verklaring inhoudende dat het onderzoek naar jihadistische websites plaatsvindt binnen de kaders van de Wiv 2002.[17] De diensthoofden van de AIVD en de MIVD verzorgden tevens op 18 december een 'technische briefing' voor de vaste commissie voor binnenlandse zaken van de Tweede Kamer. Tijdens deze openbare bijeenkomst hebben de beide diensthoofden een presentatie verzorgd over de verwerking van telecommunicatiegegevens en vragen van de Kamercommissie beantwoord.

In een uitzending van het programma Nieuwsuur op 13 januari 2014 werd gesteld dat het Amerikaanse ministerie van Defensie eigen apparatuur zou hebben staan in Burum (Friesland). In Burum staan de satellietschotels van de Nederlandse Sigint Organisatie (NSO), waarmee satellietverkeer onderschept wordt ten behoeve van de AIVD en de MIVD. Naast het terrein van de NSO zouden de Amerikanen, op het terrein van het internationale bedrijf Inmarsat, apparatuur hebben staan om satelliet-informatie op te vangen. Naar aanleiding van Kamervragen over deze berichtgeving lieten de ministers van BZK en Defensie weten dat de AIVD en de MIVD geen aanwijzingen hebben dat er in Burum sprake is van inlichtingenactiviteiten van buitenlandse mogendheden.[18]

Op 4 februari 2014 informeerden de ministers van BZK en Defensie de Tweede Kamer per brief dat de eerder genoemde 1,8 miljoen records metadata niet door de Amerikanen zijn verzameld maar door de NSO. De gegevens zouden conform de wettelijke taakuitoefening verzameld zijn in het kader van terrorismebestrijding en militaire operaties in het buitenland, en rechtmatig zijn gedeeld met de Verenigde Staten in het licht van internationale samenwerking op deze onderwerpen. Naar aanleiding van vragen vanuit de pers benadrukte de woordvoerder van de minister van BZK dat de metadata geen betrekking hebben op mobiele telefoongesprekken, maar om radioverkeer en gesprekken van satelliettelefoons.[19] De minister van Defensie liet weten dat het nadrukkelijk niet om telefoonverkeer tussen Nederlanders gaat.

Uit het voorgaande zal duidelijk zijn dat wat is begonnen als de "PRISM-affaire" - sinds de aankondiging ervan op 5 augustus 2013 - het onderzoek van de Commissie vele nieuwe facetten heeft gekregen. De Commissie onderscheidt ten tijde van het schrijven van het onderhavige toezichtsrapport op grond van de berichtgeving twee categorieën zorgen die uit de media blijken en bij de Tweede Kamer leven ten aanzien van de activiteiten van de Nederlandse inlichtingen- en veiligheidsdiensten: (1) de AIVD en de MIVD verwerven zelf

---

[15] 'Burgers dagen Nederlandse staat voor samenwerking met NSA', *Elsevier* 6 november 2013; 'De staat moet met feiten komen over afluisteren', *NRC Handelsblad* 7 november 2013.
[16] 'AIVD hackt internetfora, tegen wet in', *NRC Handelsblad* 30 november 2013.
[17] 'Verdachte webfora zijn legitiem doelwit', 30 november 2013, www.aivd.nl.
[18] *Aanhangsel Handelingen II* 2013/14, nr. 1084.
[19] 'Nederland verzamelde zelf telefoondata' en 'Ook coalitie kritisch op Plasterk over afluisteren', 5 februari 2014, www.nu.nl.

grootschalig en ongericht internet- en telefoonverkeer; (2) de AIVD en de MIVD werken (nauw) samen met de NSA en mogelijk ook andere buitenlandse diensten en hebben in dit kader (a) gebruik gemaakt van in strijd met de Nederlandse wet verzamelde telecommunicatiegegevens en/of (b) op enigerlei wijze medewerking verleend aan het verzamelen van telecommunicatiegegevens in strijd met de Nederlandse wet.

De Commissie heeft er binnen de kaders van haar aangekondigde onderzoek naar gestreefd zo volledig mogelijk tegemoet te komen aan de vragen die in de samenleving worden gesteld over de activiteiten van de AIVD en de MIVD. Daarbij stond zij voor de keuze zich, bij het onderzoek naar de samenwerking met buitenlandse diensten, ofwel specifiek te richten op de samenwerking van de AIVD en de MIVD met de NSA, ofwel in een breder perspectief aandacht te besteden aan de uitwisseling van verzamelingen gegevens in nauwe samenwerkingsrelaties tussen de Nederlandse diensten en buitenlandse diensten. De Commissie heeft voor de laatstgenoemde optie gekozen, omdat zij van oordeel is dat de focus alleen op de NSA te nauw is. De door de Tweede Kamer aan de Commissie gestelde vragen over de inzet van op de persoonlijke levenssfeer inbreukmakende bevoegdheden ten behoeve van internationale samenwerkingspartners – zowel door als voor de Nederlandse diensten – en over het uitwisselen van *big data* in internationaal verband kunnen alleen naar behoren beantwoord worden wanneer in kaart wordt gebracht op welke wijze de AIVD en de MIVD structureel samenwerken met hun samenwerkingspartners.

Bepaalde onderwerpen die in dit toezichtsrapport aan de orde komen geven aanleiding tot nader diepgaand onderzoek. De Commissie wijst erop dat zij zich reeds enige tijd bezighoudt met diepte- en vervolgonderzoeken naar de inzet van de afluisterbevoegdheid en van de bevoegdheid tot de selectie van sigint (signals intelligence) door de AIVD (een doorlopend onderzoek),[20] met het onderzoek naar de onderzoeksactiviteiten van de AIVD op sociale media,[21] de samenwerking met buitenlandse diensten door de MIVD[22] en de samenwerking met buitenlandse diensten door de AIVD.[23] De Commissie is voornemens in de eerste helft van 2014 tevens een (doorlopend) vervolgonderzoek in te stellen naar de inzet van het middel sigint door de MIVD.

Een deel van de vragen die de Tweede Kamer aan de Commissie heeft gesteld is juridisch van aard. Het gaat om de vragen welke ruimte de Wiv 2002 biedt voor bepaalde activiteiten van de diensten, wat de relatie is tussen de artikelen 24-27 en 59 Wiv 2002 en hoe de normen uit de Nederlandse Grondwet (Gw) en het Europees Verdrag voor bescherming van de Rechten van de Mens (EVRM) zich verhouden tot bepaalde activiteiten van de diensten. Deze vragen worden beantwoord in de juridische bijlage bij dit toezichtsrapport dat een uitgebreid juridisch kader bevat voor gegevensverwerking door de AIVD en de MIVD.

---

[20] Het onderzoek betreffende de periode van september 2012 tot en met augustus 2013 is aangekondigd per brief van 17 september 2012 aan de voorzitters van beide Kamers der Staten-Generaal. Het toezichtsrapport betreffende dit onderzoek zal naar verwachting begin april 2014 worden voorgelegd aan de minister. Dit geschiedt conform artikel 79, tweede lid, Wiv 2002.

[21] Aangekondigd per brief van 2 oktober 2013 aan de voorzitters van beide Kamers der Staten-Generaal. Het toezichtsrapport betreffende dit onderzoek zal naar verwachting begin april 2014 worden voorgelegd aan de minister. Dit geschiedt conform artikel 79, tweede lid, Wiv 2002.

[22] Aangekondigd per brief van 27 oktober 2007 aan de voorzitters van beide Kamers der Staten-Generaal.

[23] Aangekondigd per brief van 27 maart 2013 aan de voorzitters van beide Kamers der Staten-Generaal.

Dit toezichtsrapport heeft een geheime bijlage betreffende de AIVD en een geheime bijlage betreffende de MIVD. In deze geheime bijlagen worden bepaalde onderwerpen die in het toezichtsrapport aan de orde komen uitgebreider besproken. Tevens komen enkele onderwerpen aan de orde die vanwege hun staatsgeheime karakter niet in het toezichtsrapport behandeld kunnen worden. Ten aanzien van deze onderwerpen heeft de Commissie geen onrechtmatigheden geconstateerd. Wel heeft zij ten aanzien van drie onderwerpen die niet in het toezichtsrapport aan de orde komen aanbevelingen gedaan in de geheime bijlagen. Drie van deze aanbevelingen betreffen werkwijzen van de AIVD en twee (samenhangende) aanbevelingen betreffen een werkwijze van de MIVD.

De Commissie heeft haar onderzoek in november 2013 afgerond en het toezichtsrapport opgesteld op 18 december 2013. De ministers van BZK en Defensie zijn conform artikel 79 Wiv 2002 in de gelegenheid gesteld te reageren op de in het toezichtsrapport opgenomen bevindingen. De reacties van de ministers van BZK en Defensie zijn op 14 januari 2014 respectievelijk 15 januari 2014 door de Commissie ontvangen. Deze reacties hebben geleid tot enkele aanpassingen in het toezichtsrapport, de juridische bijlage en de geheime bijlagen, waarna het toezichtsrapport op 5 februari 2014 is vastgesteld.

2 Het onderzoek van de Commissie

Met het oog op de aard van de aan haar voorgelegde vragen en het tijdsbestek voor het onderzoek heeft de Commissie ervoor gekozen zich in dit onderzoek te richten op het in kaart brengen van de werkwijzen[24] van de diensten bij het verwerken van gegevens op het gebied van telecommunicatie en te beschrijven hoe deze werkwijzen zich verhouden tot de Wiv 2002. Daarmee verbandhoudend heeft de Commissie getoetst in hoeverre de werkwijzen van de diensten zich verdragen met de bescherming van de persoonlijke levenssfeer. Het vorenstaande betekent dat de Commissie, nog niet in concrete gevallen heeft getoetst in hoeverre voldaan is aan de daarvoor geldende wettelijke vereisten. In de loop van haar onderzoek constateerde de Commissie dat op korte termijn behoefte was aan een diepgaand onderzoek ten aanzien van concrete gevallen waarin de AIVD activiteiten verrichtte op sociale media. Zij heeft hier invulling aan gegeven binnen het onderzoek dat zij thans uitvoert naar de onderzoeksactiviteiten van de AIVD op sociale media. Ook binnen het lopende onderzoek naar de inzet van de afluisterbevoegdheid en van de bevoegdheid tot de selectie van sigint door de AIVD betreffende de periode van september 2012 tot en met augustus 2013 wordt ten aanzien van concrete gevallen onderzoek gedaan naar onderwerpen die in dit toezichtsrapport aan de orde komen.

Om een breed beeld te verkrijgen van gegevensverwerking door de AIVD en de MIVD op het gebied van telecommunicatie heeft de Commissie onderzoek gedaan naar de verschillende vormen van verwerving van telecommunicatiegegevens en het gebruik daarvan binnen de dienst. Daarbij heeft de Commissie extra aandacht gehad voor de verwerking van verzamelingen gegevens.

Bij het deel van het onderzoek dat ziet op de samenwerking van de AIVD en de MIVD met buitenlandse diensten heeft de Commissie zich de vraag gesteld welke aspecten van deze samenwerking relevant zijn. Gezien de vragen die in de afgelopen maanden in de media en de politiek naar voren zijn gekomen, heeft de Commissie ervoor gekozen zich te

[24] Onder werkwijze verstaat de Commissie niet alleen het schriftelijk beleid van de dienst, maar ook de werkwijze die in de praktijk wordt gehanteerd.

concentreren op het uitwisselen van verzamelingen ruwe gegevens door inlichtingen- en veiligheidsdiensten. Een dergelijke uitwisseling zou namelijk een aanwijzing kunnen zijn dat er sprake is van het door inlichtingen- en veiligheidsdiensten over en weer aanvullen van elkaars bevoegdheden. Daarmee zouden nationale wettelijke kaders kunnen worden omzeild. De Commissie heeft daarom onderzoek gedaan naar het door de AIVD en/of de MIVD verstrekken of ontvangen van verzamelingen (ruwe) gegevens op het gebied van telecommunicatie.

Voor zover sprake is van de uitwisseling van verzamelingen (ruwe) gegevens, betreft dit een verregaande vorm van samenwerking. Dergelijke uitwisselingen vinden plaats binnen hechte samenwerkingsrelaties. De Commissie heeft haar onderzoek daarom tot deze samenwerkingsrelaties beperkt. Zij is ervan overtuigd dat zij hiermee een goed beeld heeft verkregen van de relevante activiteiten van de diensten.

Bij haar onderzoek heeft de Commissie zich ten eerste door middel van schriftelijke vragen aan beide diensten een algemeen beeld gevormd van de materie, teneinde te bezien hoe het onderzoek het beste kon worden ingericht. Naar aanleiding van de beantwoording van deze vragen en oriënterende gesprekken met de beide diensten heeft de Commissie per dienst onderzoeksdagen gepland. Op deze onderzoeksdagen heeft de Commissie uitgebreid en in detail met de betrokken medewerkers, in de meeste gevallen hoofden van de verwervende afdelingen, gesproken over de vormen van gegevensverwerving waar de desbetreffende afdeling zich mee bezighoudt en de opslag en ontsluiting van deze gegevens voor gebruik binnen de diensten. Aansluitend is aan de Commissie getoond hoe de applicaties die gebruikt worden voor de ontsluiting van de gegevens werken en welke mogelijkheden deze applicaties bieden. Na afloop van deze onderzoeksdagen heeft de Commissie aanvullende vragen gesteld aan de diensten die ofwel schriftelijk ofwel door middel van een tweede gesprek met de betrokken gesprekspartners zijn beantwoord. De samenwerking van de AIVD en de MIVD met buitenlandse diensten is niet alleen aan bod gekomen tijdens de onderzoeksdagen van de Commissie maar is ook separaat besproken. De Commissie heeft daarnaast aanvullend onderzoek gedaan in de systemen van de diensten.

Het toezichtsrapport is als volgt opgebouwd. In de paragrafen 3 t/m 5 worden de verschillende soorten gegevensverwerking door de diensten op het gebied van telecommunicatie behandeld: de verwerking van gegevens (paragraaf 3), het gebruik van gegevens (paragraaf 4) en de uitwisseling van gegevens met buitenlandse diensten (paragraaf 5). Paragraaf 6 bevat de belangrijkste conclusies en de aanbevelingen van de Commissie.

3 De verwerving van gegevens op het gebied van telecommunicatie door de AIVD en de MIVD

3.1 Inleiding

In deze paragraaf worden de *middelen* besproken waarmee de AIVD en de MIVD gegevens op het gebied van telecommunicatie verwerven; het (laten) plaatsen van telefoontaps, interceptie en selectie van sigint, de inzet van menselijke bronnen, het binnendringen in geautomatiseerde werken (hacken) en het opvragen van telefonieverkeersgegevens en/of

gebruikersgegevens bij telecomproviders.[25] Dit zijn de meest gebruikte methoden voor het verwerven van telecommunicatiegegevens door de diensten.[26] Het is echter altijd mogelijk dat sporadisch op andere wijze telecommunicatiegegevens worden verworven. Een theoretisch voorbeeld is dat de dienst bij het binnentreden in een woning een gespecificeerde telefoonrekening van een onderzoekssubject aantreft. Ook komt het voor dat de diensten bij hun werkzaamheden ten behoeve van hun veiligheidsbevorderende taak de beschikking krijgen over telecommunicatiegegevens. Uiteraard raadplegen de diensten ook openbaar toegankelijke databases op het internet, zoals de telefoongids en de RIPE database (uitgegeven IP-adressen). Gegevens op het gebied van telecommunicatie kunnen daarnaast afkomstig zijn van buitenlandse diensten.

De meest voor de hand liggende methode om telecommunicatiegegevens te verwerven is het *onderscheppen van telecommunicatie* terwijl deze onderweg is van de verzender naar de ontvanger. De diensten beschikken over verschillende bevoegdheden die dit in bepaalde gevallen mogelijk maken. De wet maakt daarbij een onderscheid tussen telecommunicatie die via een kabel verloopt en telecommunicatie die niet-kabelgebonden is, hetgeen inhoudt dat deze via satellieten of radiogolven verloopt. Bij kabelgebonden telecommunicatie is slechts gericht aftappen toegestaan, terwijl bij niet-kabelgebonden telecommunicatie zowel gericht als ongericht[27] intercepteren is toegestaan met dien verstande dat bij het ongericht intercepteren en opnemen van niet-kabelgebonden telecommunicatie pas kennis mag worden genomen van de inhoud van de communicatie nadat toestemming is verkregen van de desbetreffende minister voor selectie van die communicatie uit de ongericht geïntercepteerde 'bulk'. Communicatie die onderweg is van verzender naar ontvanger bevindt zich in de zogenaamde transportfase en valt als zodanig onder het telefoon- en telegraafgeheim van artikel 13, tweede lid, Gw. Inbreuk op dit recht is alleen geoorloofd in de gevallen bij de wet bepaald door of met machtiging van hen die daartoe bij de wet zijn aangewezen. Het vereiste dat er toestemming dient te zijn van de verantwoordelijke minister om kennis te nemen van de inhoud van telecommunicatie die is afgetapt of geïntercepteerd, vormt hiervan de invulling.

Een andere methode is het *verwerven van opgeslagen telecommunicatiegegevens*. Dit kan gebeuren door middel van toegang tot een geautomatiseerd werk of door middel van toegang tot een andere plek waar de gegevens zijn opgeslagen. De bevoegdheden die de diensten het voornamelijk aanwenden om opgeslagen telecommunicatiegegevens te verwerven zijn de hackbevoegdheid en de bevoegdheid menselijke bronnen in te zetten. Ingevolge artikel 13 Gw vallen opgeslagen telecommunicatiegegevens niet onder het

---

[25] De Commissie besteedt bij deze beschrijving geen aandacht aan de inzet van microfoons, omdat dit niet valt onder het begrip telecommunicatie.

[26] Zie voor een bespreking van het algemene wettelijke kader voor gegevensverwerking, onder meer de vereisten van doelbinding, noodzakelijkheid en behoorlijkheid, paragrafen III en IV van de juridische bijlage bij dit toezichtsrapport en voor een bespreking van de wettelijke waarborgen bij de inzet van bijzondere bevoegdheden, onder meer de vereisten van noodzakelijkheid, proportionaliteit en subsidiariteit, paragraaf III van de juridische bijlage bij dit toezichtsrapport. De bijzondere bevoegdheden op het gebied van telecommunicatie worden in paragraaf V.2 van de juridische bijlage bij dit toezichtsrapport afzonderlijk toegelicht.

[27] In de memorie van toelichting op het wetsvoorstel Wiv 2002 wordt toegelicht dat hiermee wordt bedoeld dat de interceptie zich niet richt op berichten die afkomstig zijn van een bepaalde persoon of organisatie dan wel gerelateerd zijn aan een technisch kenmerk, maar dat bijvoorbeeld al het berichtenverkeer dat via een bepaald satellietkanaal of een op bepaalde frequentie wordt verzonden als het ware uit de ether wordt «gezogen» en vervolgens in computers wordt opgeslagen (*Kamerstukken II* 1997/98, 25 877 nr. 3, p. 44).

telegraaf- en telefoongeheim. In de toekomst zal dit mogelijk veranderen; het voorstel tot wijziging van artikel 13 Gw plaatst ook opgeslagen telecommunicatiegegevens onder het telecommunicatiegeheim (zie de juridische bijlage bij dit toezichtsrapport, paragraaf II.3).

De derde categorie verwervingsmethoden is het *opvragen van telecommunicatiegegevens* bij aanbieders van openbare telecommunicatienetwerken en openbare telecommunicatiediensten (hierna: telecomproviders) of het Centraal Informatiepunt Onderzoek Telecommunicatie (CIOT).

3.2 Telefoon- en internettaps

3.2.1 Algemeen

Een telefoontap levert de diensten verschillende soorten gegevens op: audiobestanden van de gevoerde gesprekken, tekstbestanden met de inhoud van sms-berichten en de metagegevens van gesprekken en sms-berichten. Bij deze metagegevens gaat het onder andere om de bij het telefoongesprek of het sms-bericht betrokken nummers, de starttijd en de eindtijd van het gesprek en de gegevens van de betrokken telefoonmasten.

Bij een internettap kan kennis worden genomen van de pakketjes data die verzonden of ontvangen zijn vanaf het desbetreffende IP-adres en van de metagegevens van de internetsessies. De datapakketjes kunnen betrekking hebben op bekeken internetpagina's, verzonden of ontvangen e-mails en/of chatverkeer. De metagegevens van een internetsessie zien onder andere op de tijdstippen waarop de datapakketjes zijn verzonden of ontvangen en de betrokken IP-adressen (zie de juridische bijlage bij dit toezichtsrapport, paragraaf V.2.3).

3.2.2 De toestemming voor telefoon- en internettaps

Het tappen van telefoongesprekken en internetverkeer geschiedt door beide diensten op basis van lasten; toestemming van de desbetreffende minister het telefoon- of internetverkeer van- en naar een bepaald telefoonnummer of IP-adres (dan wel meerdere nummers/IP-adressen) behorend bij een bepaalde persoon of organisatie af te luisteren. Daarbij kan het voorkomen dat ofwel de identiteit van de gebruiker ofwel het telefoonnummer of IP-adres waar een bepaalde persoon gebruik van maakt nog niet bekend zijn. Ingevolge artikel 25, zesde lid, van de Wiv 2002 behoeft dit niet in de weg te staan aan het verkrijgen van toestemming voor de tap. Wel dienen de ontbrekende gegevens zo spoedig mogelijk te worden aangevuld. Ondanks het ontbreken van de identiteit dient uiteraard wel duidelijk te zijn dat het afluisteren van de desbetreffende communicatie van belang is voor een goede taakuitoefening van de dienst.

In het verzoek om toestemming van de minister motiveren de diensten waarom zij het aftappen van de communicatie van deze persoon dan wel organisatie conform het noodzakelijkheids-, proportionaliteits- en subsidiariteitsvereiste achten ter uitvoering van bepaalde wettelijke taken (zie de juridische bijlage bij dit toezichtsrapport, paragraaf III). Wanneer toestemming is verkregen van de minister voor de telefoon- of internettap,[28] richten de diensten een verzoek aan de desbetreffende telecomprovider medewerking te verlenen aan het aftappen van de telecommunicatie. Telecomproviders zijn verplicht medewerking te

[28] Onder een internettap wordt in dit verband ook een datatap begrepen, hetgeen een tap op het internetverkeer vanaf een smartphone inhoudt.

verlenen aan een dergelijk verzoek (artikel 13.2 Telecommunicatiewet). Deze werkwijze van de diensten, waarbij er pas een verzoek aan de telecomprovider wordt opgesteld wanneer er een door de minister goedgekeurd verzoek om toestemming gericht op de desbetreffende persoon of organisatie beschikbaar is, bewerkstelligt dat de waarborgen voor de bescherming van de persoonlijke levenssfeer die zijn neergelegd in de Wiv 2002 ook in de praktijk worden gehandhaafd. De Commissie constateert dat er bij telefoon- en internettaps geen sprake is van het ongericht verwerven van (verzamelingen) gegevens.

De inzet van telefoon- en internettaps door de AIVD in individuele gevallen vormt al jaren onderwerp van een doorlopend diepteonderzoek van de Commissie. Uit dit onderzoek komt naar voren dat er geen sprake is van structurele tekortkomingen bij de uitoefening van de tapbevoegdheid door de AIVD. Gedurende de jaren 2008 – 2011 heeft de Commissie tevens de relatief beperkte uitoefening van de tapbevoegdheid door de MIVD gemonitord.

3.3 Interceptie en selectie van sigint

3.3.1 Algemeen

Het is de AIVD en de MIVD op basis van de Wiv 2002 toegestaan ongericht niet-kabelgebonden telecommunicatie te intercepteren. De diensten beschikken niet over deze bevoegdheid ten aanzien van kabelgebonden telecommunicatie. De werkwijze van de diensten bij het verwerven van gegevens uit niet-kabelgebonden communicatie is volledig anders dan bij telefoon- en internettaps (zie de juridische bijlage bij dit toezichtsrapport, paragraaf V.2.5). Het gaat hierbij om inlichtingen die verzameld worden uit opgevangen satelliet- en/of radiosignalen; *signals intelligence* oftewel sigint. Het deel van sigint dat betrekking heeft op de communicatie tussen twee partijen wordt *communications intelligence* (comint) genoemd. De AIVD richt zich bij het verwerven van sigint alleen op comint, terwijl de MIVD daarnaast ook *electronic intelligence* (elint) uit bijvoorbeeld radarsignalen verwerft. De laatstgenoemde vorm van sigint valt buiten het onderhavige onderzoek, omdat het geen (tele)communicatie betreft.

Sigint bestaat uit analoge en digitale datastromen. De analoge stroom bevat telefonie- en faxverkeer. De digitale stroom die via het internet verloopt (IP) bevat telefonieverkeer (VOIP), faxverkeer (FOIP) en ander internetverkeer. Beide stromen bevatten zowel de inhoud van de communicatie als metagegevens. Sigint-metagegevens verschaffen in ieder geval informatie over de telefoonnummers of IP-adressen betrokken bij de communicatie, het tijdstip en de duur van het gesprek. In bepaalde gevallen zijn ook geografische gegevens beschikbaar.

3.3.2 De ongerichte interceptie door de NSO

De ongerichte interceptie wordt ten behoeve van de AIVD en de MIVD uitgevoerd door de Nationale Sigint Organisatie (NSO), die door beide diensten wordt aangestuurd en beheersmatig is ingebed bij de MIVD. De activiteiten van de NSO richten zich op satelliet- en/of radiocommunicatie. De Commissie stelt vast dat hierbij geen sprake is van de interceptie van kabelgebonden telecommunicatie. Bij de verwerving van communicatie die via satellieten verloopt, intercepteert de NSO bundels die bestaan uit vele communicatiesessies. Deze verwerving is ongericht, want op dat moment is niet bekend van welke personen de communicatie wordt onderschept. Bij *high frequency* (HF) radioverkeer is het voor de NSO mogelijk om de frequentie te achterhalen waarop een bepaalde persoon of

organisatie uitzendt en op die manier gericht de communicatie van deze persoon of organisatie te intercepteren.

Het is om technische en financiële redenen in het belang van de diensten de ongerichte interceptie van satellietverkeer af te bakenen, zodat het verworven materiaal zo min mogelijk irrelevante communicatiesessies bevat. Hiervoor bestaan verschillende mechanismen. De NSO verkent de ether op basis van de behoeftestelling vanuit de diensten door gebruik te maken van de bevoegdheid om te *searchen* die is geregeld in artikel 26 Wiv 2002. Hiervoor is geen toestemming van de minister vereist (zie de juridische bijlage bij dit toezichtsrapport, paragraaf V.2.4). De wetgever heeft op dit punt overwogen dat het searchen er niet op is gericht van de inhoud van de telecommunicatie kennis te nemen en voorts dat een toestemmingsvereiste geen toegevoegde waarde zou hebben omdat van tevoren niet gericht gemotiveerd zou kunnen worden waarnaar gezocht wordt.[29]

Aanvullend aan de verkenning van de ether door middel van de searchbevoegdheid worden bij de interceptie van satellietverkeer *filters* ingezet door de NSO ten behoeve van de diensten. De AIVD en de MIVD gaan bij het (laten) filteren van het satellietverkeer verschillend te werk.

Ten behoeve van de AIVD scheidt de NSO het digitale verkeer van het analoge verkeer. Bij digitaal verkeer, dat uit grotere bestanden bestaat dan het analoge verkeer en bovendien een enorme hoeveelheid gegevens betreft, worden de metagegevens gescheiden van de inhoud. De relevante inhoud van het digitale verkeer wordt al direct bij interceptie geselecteerd aan de hand van zogenaamde *leads* en lasten. Alleen deze inhoud wordt geïntercepteerd en naar de AIVD gestuurd. Dit betekent dat de inhoud van digitale communicatiesessies slechts wordt verworven door de AIVD als er ofwel toestemming van de minister is verkregen voor de selectie op een bepaalde identiteit, technisch kenmerk of trefwoord, ofwel als bepaalde kenmerken of trefwoorden door een van de operationele teams zijn opgegeven als *lead*. De AIVD werkt met *leads* als invulling van de searchbevoegdheid ingevolge artikel 26 Wiv 2002. Wanneer een medewerker van een van de operationele teams de communicatie behorend bij een bepaald kenmerk of trefwoord relevant acht voor een onderzoek van het team, kan deze ervoor kiezen het kenmerk of trefwoord op te nemen op de *leadl*ijst voor de NSO zodat daar bij het intercepteren op kan worden gefilterd. Hiervoor is op grond van het beleid van de AIVD geen toestemming van een leidinggevende vereist. Hierbij dient te worden opgemerkt dat volgens het beleid van de AIVD op basis van een *lead* geen kennis mag worden genomen van de inhoud van geïntercepteerde communicatie ten behoeve van het operationeel proces. Voor het gebruik ten dienste van het operationeel proces wordt de *lead* omgezet in een last, waarvoor toestemming van de minister van BZK is vereist (zie tevens paragraaf 3.3.4 van dit toezichtsrapport).

Het overgrote deel van de kenmerken waarop in het digitale verkeer door de NSO wordt gefilterd ten behoeve van de AIVD komt voort uit lasten. De andere kenmerken komen voort uit *leads*. De analoge communicatiestromen worden niet door de NSO gefilterd ten behoeve van de AIVD; het analoge verkeer dat aanwezig is in de geïntercepteerde satellietbundels wordt verworven en integraal overgedragen aan de AIVD. Filteren wordt bij het analoge verkeer niet nodig geacht omdat het om een relatief beperkte en steeds afnemende hoeveelheid gegevens gaat. Dit omdat in toenemende mate de overstap wordt gemaakt naar digitale communicatie.

[29] *Kamerstukken II* 2000/01, 25 877, nr. 14, p. 34 en 36.

Ten behoeve van de MIVD filtert de NSO reeds bij interceptie op bepaalde technische kenmerken. Dit betekent dat alleen het satellietverkeer dat voldoet aan deze kenmerken wordt geïntercepteerd. Al het geïntercepteerde materiaal wordt vervolgens naar de MIVD gestuurd. De technische kenmerken waarop wordt gefilterd door de NSO kunnen uit verschillende bronnen afkomstig zijn, zoals eerder onderzoek door de MIVD of een openbaar toegankelijke bron. Het kunnen op een bepaalde persoon of organisatie gerichte kenmerken zijn ten aanzien waarvan reeds een selectielast is verkregen of het kunnen bredere kenmerken zijn die bijvoorbeeld zien op de regio waarbinnen de communicatie heeft plaatsgevonden. De keuzes die hierin worden gemaakt zijn afhankelijk van de behoefte, de technische mogelijkheden en de informatiepositie van de MIVD. De Commissie merkt het toepassen van deze filters aan als onderdeel van de interceptie op basis van artikel 27 Wiv 2002. Hiervoor is op basis van de Wiv 2002 geen toestemming vereist, omdat de gegevens in dit stadium alleen worden opgeslagen in afwachting van eventuele nadere verwerking.

3.3.3 Het analyseren van metagegevens

Nadat interceptie heeft plaatsgevonden vindt er doorgaans onderzoek plaats op basis van de geïntercepteerde metagegevens. Deze metagegevens worden door de diensten apart van de inhoud van de communicatie opgeslagen en met behulp van applicaties geanalyseerd. Bij de AIVD worden de metagegevens die uit sigint zijn verkregen tezamen met metagegevens uit andere bronnen geanalyseerd. Het aspect van de samenvoeging van metagegevens door de AIVD wordt nader besproken in paragraaf 4.2. De metadata-analyse die plaatsvindt kan zowel nieuwe technische kenmerken opleveren van huidige onderzoekssubjecten (personen of organisaties) als nieuwe onderzoekssubjecten. Het proces van metadata-analyse wordt door beide diensten gebruikt ter ondersteuning van het proces van sigint-verwerving en selectie.

In de loop van haar onderzoek heeft de Commissie kennisgenomen van het standpunt van medewerkers van beide diensten dat ongericht geïntercepteerde metagegevens niet eerst geselecteerd behoeven te worden op basis van een last ingevolge artikel 27, derde lid, Wiv 2002 alvorens deze worden geanalyseerd. Metagegevens worden door de diensten namelijk aangemerkt als 'lastenvrij'. Door de diensten wordt gesteld dat bij metadata-analyse geen kennis wordt genomen van de inhoud van de communicatie, waardoor toestemming van de minister niet is vereist.

De Commissie overweegt op dit punt dat in de memorie van toelichting op het wetsvoorstel Wiv 2002 inderdaad wordt geredeneerd dat geen toestemmingsvereiste ingevolge artikel 19 wordt gesteld aan het ongericht intercepteren van niet-kabelgebonden communicatie, omdat daarbij nog geen kennis wordt genomen van de inhoud en er derhalve nog geen inbreuk op de persoonlijke levenssfeer plaatsvindt, meer in het bijzonder het telefoon- en telegraafgeheim.[30] Uit de rest van deze passage blijkt echter dat men uit is gegaan van de situatie dat met de ingewonnen gegevens nog niets kan worden gedaan door de diensten.[31] Dit is thans niet meer het geval. De analyse van geïntercepteerde metagegevens die bij beide diensten plaatsvindt is bij het opstellen van de Wiv 2002 kennelijk niet voorzien door de wetgever. Het is daarom ten eerste de vraag of analyse van ongericht geïntercepteerde metagegevens is toegestaan en, indien dit het geval is, of het niet aangewezen is dat nadere vereisten worden gesteld aan deze vorm van gegevensverwerking.

[30] *Kamerstukken II* 1997/98, 25 877, nr. 3, p. 44.
[31] *Kamerstukken II* 1997/98, 25 877, nr. 3, p. 44.

In antwoord op de eerste vraag merkt de Commissie op dat het feit dat in de Wiv 2002 en de bijbehorende memorie van toelichting geen aandacht wordt besteed aan de mogelijkheid van het nader verwerken van geïntercepteerde metagegevens niet per definitie betekent dat de wet hiervoor geen ruimte biedt. Het gaat immers om de nadere verwerking van gegevens die reeds rechtmatig zijn verzameld. De Wiv 2002 bevat een algemene wettelijke basis voor gegevensverwerking (artikel 12 lid 1), waar ook metadata-analyse onder geschaard kan worden.

In antwoord op de tweede vraag dient eerst bezien te worden of metadata-analyse inbreuk maakt op de persoonlijke levenssfeer. Hiervoor moet—worden vastgesteld of de geïntercepteerde metagegevens dienen te worden aangemerkt als persoonsgegevens in de zin van de Wiv 2002: gegevens die betrekking hebben op een identificeerbare of geïdentificeerde, individuele natuurlijke persoon. Dit is niet per definitie het geval. Ten aanzien van een deel van de metagegevens kan worden geconstateerd dat deze niet herleidbaar zijn tot individuele personen. Deze metagegevens betreffen bijvoorbeeld de locatie van betrokken zendmasten of de gebruikte IP-protocollen. Hierdoor vallen deze metagegevens niet onder het bereik van artikel 10 Gw en houdt het verwerken ervan geen inbreuk in op de persoonlijke levenssfeer. Bij telefoonnummers en IP-adressen ligt dit minder eenvoudig, omdat deze gegevens onder omstandigheden wel te koppelen zijn aan bepaalde gebruikers. Uit de wetsgeschiedenis bij de Wet bescherming persoonsgegevens blijkt dat dergelijke gegevens als persoonsgegevens dienen te worden aangemerkt indien het voor de instantie die erover beschikt mogelijk is om zonder onevenredige inspanning de identiteit van de gebruiker te achterhalen.[32] De Commissie constateert dat de verzamelde metagegevens voor de diensten aanleiding kunnen vormen om vervolgstappen te zetten om de identiteit van de gebruiker te achterhalen. Het kan hierbij gaan om het opvragen van de gebruikersgegevens bij een bepaald telefoonnummer of IP-adres bij het CIOT of om het koppelen van andere informatie waar de dienst reeds over beschikt aan de metagegevens. In de optiek van de Commissie dient in ieder geval het identificeren van de gebruiker door het koppelen van gegevens die reeds binnen de diensten beschikbaar zijn aan de metagegevens aangemerkt te worden als het zonder onevenredige inspanning achterhalen van diens identiteit. De conclusie is derhalve dat een deel van de metagegevens die de diensten ongericht intercepteren dient te worden geclassificeerd als persoonsgegevens.

Aangezien metagegevens worden beschermd door artikel 10 Gw voor zover het om persoonsgegevens gaat, stelt de Commissie vast dat het verwerken van ongericht geïntercepteerde metagegevens in bepaalde gevallen een inbreuk vormt op de persoonlijke levenssfeer van de betrokkenen. In het licht van deze vaststelling acht zij het van belang dat het proces van metadata-analyse bij wet wordt voorzien van waarborgen die beschermen tegen ongeoorloofde inbreuken op de persoonlijke levenssfeer zoals het motiveren van de noodzakelijkheid, proportionaliteit en subsidiariteit van de gegevensverwerking ten behoeve van het verkrijgen van interne dan wel externe toestemming daarvoor (zie de juridische bijlage bij dit toezichtrapport, paragraaf III).[33] Deze waarborgen zijn thans niet aanwezig in het proces van metadata-analyse na ongerichte interceptie. De Commissie beveelt aan een specifieke regeling voor de verwerking van metagegevens op te nemen in de wet.

[32] *Kamerstukken II* 1997/98, 25 892, nr. 3, p. 47.

[33] In de recente evaluatie van de Wiv 2002 is door de Commissie-Dessens een nieuw stelsel van interceptiebepalingen voorgesteld waarin ook metadata-analyse een plaats heeft gekregen.

3.3.4 Het searchen en het plegen van selectie

Nadat door de diensten - eventueel door middel van metadata-analyse - technische kenmerken zijn onderkend waarvan vermoed wordt dat zij gerelateerd zijn aan onderzoekssubjecten van de dienst of die behoren bij nieuwe onderzoekssubjecten, wordt in bepaalde gevallen de searchbevoegdheid ingezet om vast te stellen of het inderdaad om communicatie van het desbetreffende onderzoekssubject gaat en bij nieuwe onderzoekssubjecten om de identiteit vast te stellen en te bezien of er inderdaad een relatie met het onderzoeksveld bestaat. Het gaat hierbij om search ten behoeve van selectie.

In haar toezichtsrapport betreffende de inzet van sigint door de MIVD beoordeelde de Commissie drie gangbare praktijken van de MIVD bij het searchen ten behoeve van selectie:

1. Het *searchen* van de bulk aan communicatie om te bepalen of met de selectiecriteria waarvoor toestemming is verkregen de gewenste informatie kan worden gegenereerd;
2. Het *searchen* van de bulk aan communicatie om potentiële 'targets' te identificeren of te duiden;
3. Het *searchen* van de bulk aan communicatie naar gegevens waaruit, in het kader van een verwacht nieuw onderzoeksgebied, toekomstige selectiecriteria kunnen worden afgeleid.

De eerste vorm van searchen houdt in dat aan de hand van informatie over personen en organisaties die reeds als onderzoekssubject zijn aangemerkt en voor de selectie van wier gegevens reeds toestemming is verleend door de minister wordt gezocht naar technische kenmerken die aan de desbetreffende personen en organisaties toebehoren. De tweede en de derde vorm van searchen richten zich op het onderkennen, duiden en identificeren van nieuwe onderzoekssubjecten, ofwel binnen lopende onderzoeken (de tweede vorm van searchen), ofwel binnen verwachte nieuwe onderzoeksgebieden (de derde vorm van searchen). De Commissie heeft in haar bovengenoemde toezichtsrapport alleen de eerstgenoemde vorm van searchen ten behoeve van selectie rechtmatig geacht, omdat alleen bij die vorm van searchen de inbreuk op de persoonlijke levenssfeer wordt ondervangen door de toestemming van de minister ten aanzien van de desbetreffende persoon of organisatie selectie te plegen. De inzet van de searchbevoegdheid is hierbij *ondersteunend* aan de inzet van de selectiebevoegdheid waarvoor toestemming is verkregen.[34] Dit is noodzakelijk, omdat artikel 13 Gw een machtiging door een bevoegd orgaan vereist voordat inbreuk mag worden gemaakt op het telefoon- en telegraafgeheim. De Commissie gaf de wetgever in het genoemde toezichtsrapport in overweging te bezien of het, met inachtneming van de bescherming van de persoonlijke levenssfeer, noodzakelijk is dat aan de MIVD (en de AIVD) de bevoegdheid wordt toegekend te searchen ten behoeve van een nieuwe inzet van de selectiebevoegdheid.

Uit de gesprekken die de Commissie heeft gevoerd is naar voren gekomen dat de MIVD de searchbevoegdheid toepast ten aanzien van nieuwe onderzoekssubjecten naar aanleiding van metadata-analyse. Dit betreft de tweede vorm van search ten behoeve van selectie; een werkwijze die de Commissie in haar eerdere toezichtsrapport inzake de inzet van sigint door de MIVD onrechtmatig achtte. Hieruit blijkt dat de problemen die de Commissie in haar eerdergenoemde toezichtsrapport signaleerde ten aanzien van de toepassing van de searchbevoegdheid door de MIVD in ieder geval voor een deel nog bestaan.

---

[34] Toezichtsrapport van de CTIVD nr. 28 inzake de inzet van Sigint door de MIVD, *Kamerstukken II* 2011/12, 29 924, nr. 74 (bijlage), beschikbaar op www.ctivd.nl, paragrafen 4.3.3 en 7.4.3.

Op de werkwijze van de AIVD inzake het searchen zal worden teruggekomen in het doorlopende onderzoek van de Commissie naar de inzet van de afluisterbevoegdheid en van de bevoegdheid tot de selectie van sigint door de AIVD. Het toezichtsrapport betreffende dit onderzoek over de periode van september 2012 tot en met augustus 2013 zal naar verwachting begin april 2014 worden voorgelegd aan de minister.

Bij beide diensten wordt de searchbevoegdheid in het geïntercepteerde materiaal ten behoeve van de selectie uitgevoerd door een beperkt aantal medewerkers van de verwervende afdeling, die niet betrokken zijn bij de inhoudelijke analyse van inlichtingen. Indien de kenmerken die bij het searchen zijn gebruikt inderdaad inhoudelijke communicatie opleveren, dient er toestemming van de minister aanwezig te zijn voor de selectie van het materiaal alvorens de inhoud van de communicatie beschikbaar komt voor gebruik in het operationele proces. Deze werkwijze is bij beide diensten technisch ingebed.

De Commissie heeft al in eerdere toezichtsrapporten vastgesteld dat zowel de AIVD als de MIVD de inzet van de selectiebevoegdheid onvoldoende motiveerden. Het ging hierbij – kort samengevat – om het onvoldoende toespitsen van de motivering voor de selectie op de personen en/of organisaties die in de selectielijst waren opgenomen.[35] De Commissie blijft nadrukkelijk aandacht vragen en behouden voor deze problematiek.[36]

3.4 Menselijke bronnen

3.4.1 Algemeen

Een van de middelen die de diensten tot hun beschikking hebben voor het verwerven van gegevens zijn menselijke bronnen die toegang hebben dan wel verkrijgen tot bepaalde gegevens die niet openbaar zijn (zie de juridische bijlage bij dit toezichtsrapport, paragraaf V.2.1).

Voor zover de MIVD menselijke bronnen inzet voor de verwerving van gegevens op het gebied van telecommunicatie, geeft het onderzoek van de Commissie geen aanleiding tot opmerkingen.

De activiteiten van de AIVD op dit gebied vallen uiteen in twee categorieën. Deze categorieën worden nader toegelicht in de geheime bijlage betreffende de AIVD bij dit toezichtsrapport. Onderstaand worden de bevindingen van de Commissie in algemene bewoordingen weergegeven, zonder afbreuk te doen aan de geheimhouding van bronnen, het actueel kennisniveau en/of de werkwijze van de AIVD.

3.4.2 De toestemming voor bepaalde activiteiten van menselijke bronnen

[35] Zie bijvoorbeeld het toezichtsrapport van de CTIVD nr. 28 inzake de inzet van sigint door de MIVD, paragraaf 8.3.4 en het toezichtsrapport van de CTIVD nr. 19 inzake de inzet van de afluisterbevoegdheid en de signaalinterceptie door de AIVD, *Kamerstukken II* 2008/09, 29 924, nr. 29 (bijlage), paragraaf 7, beide beschikbaar op www.ctivd.nl.

[36] In het doorlopend diepteonderzoek naar de inzet van de afluisterbevoegdheid en van de bevoegdheid tot de selectie van sigint door de AIVD 25/27 AIVD wordt hieraan aandacht besteed. De Commissie is tevens voornemens in het eerste kwartaal van 2014 een vervolgonderzoek in te stellen naar de inzet van sigint door de MIVD.

Het verwerven van gegevens door middel van een menselijke bron geschiedt op verzoek van één of meerdere van de operationele teams van de AIVD. De verwervende afdeling beziet in een voorkomend geval eerst of de gevraagde informatie kan worden verworven via een bestaande menselijke bron. Indien hiertoe geen mogelijkheid wordt gezien, wordt getracht een menselijke bron te werven die op enigerlei wijze toegang heeft tot de informatie. Wanneer gekozen wordt voor de inzet van een nieuwe menselijke bron richt, in het geval van een behoefte vanuit meerdere teams, de verwervende afdeling een verzoek om toestemming voor de inzet van een agent ingevolge artikel 21 Wiv 2002 en/of een informant ingevolge artikel 17 Wiv 2002 aan het desbetreffende unithoofd.[37] Het verschil tussen deze twee soorten menselijke bronnen is dat een agent wordt aangestuurd door de dienst, terwijl een informant in beginsel vanuit diens gebruikelijke activiteiten informatie doorgeeft.[38] Hierdoor wordt de inzet van een agent in de Wiv 2002 aangemerkt als een bijzondere bevoegdheid, terwijl de inzet van een informant onder de algemene bevoegdheid tot het verzamelen van gegevens valt.

In het verzoek om toestemming voor de inzet van een agent of een informant worden de operationele plannen toegelicht. De beoordeling van de noodzakelijkheid, proportionaliteit en subsidiariteit van het verzoek vindt inhoudelijk plaats door de verzoekende teams; de teams zijn immers in de beste positie te beargumenteren waarom de te verwerven gegevens nodig zijn voor het onderzoek en waarom de gegevens op deze wijze verworven dienen te worden. De operationele teams leveren derhalve input voor het verzoek dat de verwervende afdeling opstelt. Wanneer het gaat om gegevens ten behoeve van slechts één operationeel team, stelt het team zelf het verzoek op. Het verzoek dient vervolgens beoordeeld te worden door de juridische afdeling, voordat het ter beslissing wordt voorgelegd aan het unithoofd.

De toestemming van het unithoofd voor de inzet van een agent ingevolge artikel 21 Wiv 2002 geldt voor ten hoogste drie maanden. Wanneer vanuit het betrokken operationele team behoefte bestaat aan de voortzetting van de inzet, dient toestemming voor verlenging te worden verzocht. Dit hoeft dan niet meer op het niveau van unithoofd zoals bij de initiële inzet, maar op het niveau van teamhoofd. In een dergelijk verzoek komen de recente ontwikkelingen in de operaties aan de orde en worden operationele keuzes zo nodig herzien. Ook de toestemming voor de inzet van een informant op basis van artikel 17 Wiv 2002 dient periodiek te worden verlengd op het niveau van het teamhoofd.

De Commissie constateert dat bij de initiële inzet van een menselijke bron en daarna periodiek in het kader van de verlenging van de inzet, toestemming wordt verkregen voor het verwerven van de informatie waarop de operationele plannen zijn gericht. Zij wijst erop dat echter niet per afzonderlijke opdracht toestemming wordt gevraagd door de verwervende afdeling of het betrokken operationele team.

De Commissie overweegt dat het de taak van de AIVD is om flexibel in te spelen op nieuwe ontwikkelingen. Dit leidt ook tot het op nieuwe manieren inzetten van menselijke bronnen.

---

[37] De mandatering van de bevoegdheid om toestemming te geven voor de inzet en de verlenging van de inzet is ter uitwerking van artikel 19 Wiv 2002 vastgelegd in het Mandaatbesluit bijzondere bevoegdheden AIVD 2009. De artikelen 4 en 5 van het Mandaatbesluit zien op het vereiste niveau van toestemming voor de inzet van agenten. Uit het Mandaatbesluit blijkt overigens dat wanneer de agent een persoon betreft met een bepaalde maatschappelijke functie, het toestemmingsniveau hoger ligt. Dit kan het niveau van directeur, hoofd van dienst of minister zijn.

[38] Zie tevens het toezichtsrapport van de CTIVD nr. 8a inzake de inzet door de MIVD van informanten en agenten, meer in het bijzonder in het buitenland, *Kamerstukken II* 2005/06, 29 924, nr. 11 (bijlage), beschikbaar op www.ctivd.nl, para. 4.

Zij is van oordeel dat het in een dergelijk dynamisch veld alleen mogelijk is op adequate wijze de bescherming van de persoonlijke levenssfeer te waarborgen indien de nadruk komt te liggen op de aard van de activiteit en het type gegevens dat wordt verworven, zo onafhankelijk mogelijk van het middel waarmee de gegevens worden verworven (de inzet van de menselijke bron).[39]

In haar onderzoek is het de Commissie gebleken dat door de juridische afdeling van de AIVD een werkwijze is voorgesteld die in grotere mate tegemoet komt aan het beschermen van de persoonlijke levenssfeer. Zo wordt onder meer voorgesteld toestemming op een hoger niveau te vragen dan normaal gesproken benodigd is voor de inzet van de desbetreffende menselijke bron, wanneer deze een activiteit gaat ondernemen die vergelijkbaar is met tappen of hacken. Deze activiteit zal dan ook separaat gemotiveerd dienen te worden. Voor wat betreft reeds verzamelde gegevens wordt in de notitie geadviseerd dat deze niet vernietigd behoeven te worden op grond van artikel 43, tweede lid, Wiv 2002, omdat deze op grond van de Wiv 2002 niet onrechtmatig zijn verkregen. Het voorstel van de juridische afdeling wordt nader toegelicht in de geheime bijlage betreffende de AIVD bij dit toezichtsrapport.

De Commissie volgt de juridische afdeling niet waar het gaat om de rechtmatigheid van de huidige werkwijze in de genoemde situaties. Zij merkt op dat wanneer door menselijke bronnen bijzondere bevoegdheden worden ingezet in opdracht en onder aansturing van de AIVD, deze bevoegdheden moeten worden beschouwd als ingezet door de AIVD. Voor het tappen in de zin van artikel 25 Wiv 2002 en voor de het hacken in de zin van artikel 24 Wiv 2002, geldt derhalve ook dat deze bevoegdheden in feite door de AIVD zijn ingezet. Ingevolge de Wiv 2002 dient de minister van BZK om toestemming te worden verzocht voor het tappen. Op grond van het Mandaatbesluit bijzondere bevoegdheden AIVD 2009 dient de directeur van de eenheid om toestemming te worden verzocht voor het hacken. Het vereiste toestemmingsniveau voor de inzet van een menselijke bron ligt op het niveau van unithoofd en is daardoor lager dan gezien de aard van de activiteiten vereist is. De inzet van de bijzondere bevoegdheden dient bovendien separaat van de inzet van de menselijke bron te worden gemotiveerd. De Commissie acht het ontoelaatbaar dat deze waarborgen buiten toepassing blijven.

Bij de vaststelling van de ernst van de bovengenoemde gebreken is de Commissie van oordeel dat onderscheid dient te worden gemaakt tussen de situatie waarin ten onrechte geen toestemming is gevraagd van de minister voor een activiteit die als tappen dient te worden aangemerkt en de situatie waarin geen toestemming is gevraagd van de directeur van de eenheid voor een activiteit die als hacken dient te worden aangemerkt. Het eerstgenoemde toestemmingsniveau wordt voorgeschreven door de Wiv 2002 en vormt de invulling van het vereiste ingevolge artikel 13 Gw dat inbreuk op het telefoon- en telegraafgeheim slechts is toegestaan door of met machtiging van hen die daartoe bij de wet zijn aangewezen. Het niet naleven van dit vereiste leidt naar het oordeel van de Commissie tot onrechtmatigheid.

Het toestemmingsniveau voor het hacken volgt niet als zodanig uit de Wiv 2002, maar uit het Mandaatbesluit bijzondere bevoegdheden AIVD 2009, dat intern binnen de AIVD is vastgesteld. Nu het niet gaat om een wettelijke plicht en er sprake is van slechts één niveau

[39] Zie tevens het rapport van de Commissie-Dessens, *Evaluatie Wet op de inlichtingen- en veiligheidsdiensten 2002. Naar een nieuwe balans tussen bevoegdheden en waarborgen*, december 2013, *Kamerstukken II* 2013/14, 33 820, nr. 1 (bijlage), p. 79.

verschil (directeur of unithoofd), is de Commissie van oordeel dat deze werkwijze van de AIVD niet zonder meer als onrechtmatig valt aan te merken. Dit wil evenwel niet zeggen dat de AIVD in deze gevallen rechtmatig heeft gehandeld. De noodzakelijkheid, proportionaliteit en subsidiariteit van het hacken dienen namelijk in voldoende mate te zijn gemotiveerd, wil voldaan zijn aan de wettelijke vereisten omtrent de uitoefening van bijzondere bevoegdheden (zie de juridische bijlage bij dit toezichtsrapport, paragraaf III). Voor zover in de motivering voor de inzet of de verlenging van de menselijke bron die het hacken heeft uitgevoerd, onvoldoende aandacht is besteed aan het motiveren van het hacken, zal derhalve alsnog tot onrechtmatigheid worden geconcludeerd. In het onderzoek dat de Commissie uitvoert naar de onderzoeksactiviteiten van de AIVD op sociale media zal zij ten aanzien van concrete gevallen beoordelen of de AIVD rechtmatig heeft gehandeld. Het toezichtsrapport betreffende dit onderzoek zal naar verwachting begin april 2014 worden voorgelegd aan de minister.

De Commissie beveelt aan dat de AIVD onverwijld zijn werkwijze aanpast door voortaan het juiste toestemmingsniveau in acht te nemen en de inzet van bijzondere bevoegdheden door menselijke bronnen separaat van de inzet van de desbetreffende menselijke bronnen te motiveren.

3.5 Hacken

3.5.1 Algemeen

Beide diensten verwerven gegevens op het gebied van telecommunicatie door middel van het binnendringen in geautomatiseerde werken, ook wel hacken genoemd (zie de juridische bijlage bij dit toezichtsrapport, paragraaf V.2.2). De MIVD voert het hacken uit in samenwerking met de AIVD. Om praktische redenen komt het ook voor dat de AIVD een hack uitvoert ten behoeve van de MIVD.

Hacken kan de diensten verschillende soorten gegevens opleveren. De belangrijkste categorieën zijn e-mailaccounts en webfora. Het kan echter ook gaan om een andere soort internetsite of andere bestanden die in een geautomatiseerd werk zijn opgeslagen. Van e-mailaccounts, webfora en andere internetsites worden zowel inhoudelijke communicatie als metagegevens verworven. Een voordeel van het hacken van een e-mailaccount ten opzichte van een internettap is dat in een e-mailaccount alle e-mailverkeer vanaf verschillende IP-adressen samenkomt, terwijl bij een internettap alleen het verkeer van en naar een bepaald IP-adres of bepaalde IP-adressen wordt getapt.

3.5.2 De toestemming voor de hack

De AIVD maakt in zijn beleid onderscheid tussen het op afstand binnendringen en het binnendringen in een geautomatiseerd werk dat fysiek in handen is van de dienst (bijvoorbeeld de laptop van een onderzoekssubject). Het toestemmingsniveau dat vereist is voor de inzet van de bevoegdheid is voor het binnendringen op afstand hoger dan voor het binnendringen wanneer de AIVD het geautomatiseerde werk fysiek in handen heeft. Voor binnendringen op afstand dient er toestemming te zijn van de directeur van de eenheid.[40] Voor het binnendringen van een werk waartoe de AIVD fysieke toegang heeft, is

[40] Artikel 7, eerste lid, Mandaatbesluit bijzondere bevoegdheden AIVD 2009.

toestemming van het desbetreffende unithoofd voldoende.[41] Bij beide vormen van binnendringen in een geautomatiseerd werk wordt het verzoek opgesteld door het betrokken operationele team en dient dit verzoek beoordeeld te worden door het desbetreffende teamhoofd, de juridische afdeling en in het geval van binnendringen op afstand ook het desbetreffende unithoofd. Na het verkrijgen van toestemming wordt de hack uitgevoerd door de verwervende afdeling.

In het verzoek om toestemming dient gemotiveerd te worden welk geautomatiseerd werk het betreft en welke informatie met het hacken wordt beoogd te worden verkregen. Indien het verzoek ziet op het hacken van een e-mailaccount kan dit ook betrekking hebben op 'gerelateerde kenmerken' zodat ook een nieuw e-mailadres dat door hetzelfde onderzoekssubject wordt aangemaakt onder de toestemming valt. De juridische afdeling beoordeelt dan in een voorkomend geval of het nieuwe kenmerk onder een eerder verkregen toestemming valt.

De AIVD heeft de Commissie aangegeven dat verzoeken om toestemming soms vrij breed worden verwoord zodat de flexibiliteit wordt behouden om de bestanden te kunnen verwerven (over te nemen) waar het betrokken operationele team, na overleg, behoefte aan heeft. Hoewel de Commissie begrip heeft voor het feit dat het voor de AIVD op voorhand slechts beperkt duidelijk is welke informatie zal worden aangetroffen en het daarom voor het operationele team de voorkeur heeft meerdere mogelijkheden te hebben, acht zij het van belang dat op basis van de beschikbare informatie zo gericht mogelijk wordt gemotiveerd op welke informatie de hack is gericht. Alleen dan kan de noodzakelijkheid, proportionaliteit en subsidiariteit van de voorgenomen inzet ten volle worden beoordeeld (zie de juridische bijlage bij dit toezichtsrapport, paragraaf III). Wanneer bij het hacken door de verwervende afdeling gegevens worden aangetroffen die niet onder de toestemming vallen, maar wellicht wel relevant zijn voor het onderzoek van het operationele team, kan – via een spoedprocedure – na overleg met het operationele team alsnog toestemming worden gevraagd voor het overnemen van deze gegevens.

De MIVD verzoekt in voorkomende gevallen de minister van Defensie toestemming voor de inzet van de bevoegdheid tot hacken. Voor verlenging van de inzet is toestemming het hoofd van de MIVD vereist. Het verzoek wordt voorafgaand beoordeeld door het hoofd van de verwervende afdeling, de juridische afdeling en de (plaatsvervangende) directeur van de MIVD.

3.5.3 De toestemming voor bepaalde hackactiviteiten door de AIVD

Binnen de AIVD heeft een juridische discussie plaatsgevonden over het geëigende toestemmingsniveau voor de inzet van de hackbevoegdheid in bepaalde gevallen. De juridische afdeling heeft ten aanzien van de toepassing van de hackbevoegdheid twee aandachtspunten gesignaleerd:

[41] Ingevolge artikel 7, tweede lid, Mandaatbesluit bijzondere bevoegdheden AIVD 2009 had ook voor toestemmingverlening door de directeur van de desbetreffende eenheid kunnen worden gekozen.

1) De inzet van een hack leidt in veel gevallen tot het, kennisnemen van stromende informatie.[42] Op grond van het Mandaatbesluit bijzondere bevoegdheden AIVD 2009 dient hiervoor toestemming van de minister van BZK te worden verkregen;
2) bij de inzet van een hack is van tevoren niet altijd (goed) te overzien waartoe dit qua opbrengst leidt en hoe groot de potentiële inbreuk op de persoonlijke levenssfeer zal zijn. Geregeld blijkt deze gelijk aan die van een tap te zijn.

Als oplossing wordt aangedragen dat de juridische afdeling erop dient toe te zien dat conform het Mandaatbesluit bijzondere bevoegdheden AIVD 2009 toestemming van de minister wordt gevraagd, wanneer voorzienbaar is of beoogd wordt dat door middel van de hack kennis wordt genomen van gesprekken, telecommunicatie en/of gegevensoverdracht in de zin van artikel 25 Wiv 2002. Daarnaast wordt voorgesteld om uit oogpunt van zorgvuldigheid ook toestemming aan de minister te vragen indien van tevoren niet kan worden uitgesloten dat door middel van een hack kennis zal worden genomen van gesprekken, telecommunicatie of gegevensoverdracht. Tot slot stelt de juridische afdeling voor om de lopende hacks indachtig de voornoemde aandachtspunten te beoordelen.

De Commissie constateert dat het eerdergenoemde mandaatbesluit aansluit bij het wettelijke vereiste dat toestemming dient te worden verleend door de minister in het geval van hackactiviteiten waarmee kennis wordt genomen van stromende telecommunicatie. Hiermee wordt tevens aangesloten bij het telefoon- en telegraafgeheim op grond van artikel 13, tweede lid, Gw in zijn huidige vorm. Voor zover geen toestemming is gevraagd van de minister in dergelijke gevallen, is de Commissie van oordeel dat dit onrechtmatig is. Zij beveelt aan dat de AIVD onverwijld zijn werkwijze in overeenstemming brengt met het wettelijke vereiste dat er toestemming dient te worden gevraagd aan de minister van BZK wanneer kennis wordt genomen van stromende telecommunicatie in de zin van artikel 25 Wiv 2002.

De Commissie wijst er bovendien op dat het voorstel voor het nieuwe artikel 13 Gw consequenties heeft voor de hackbevoegdheid (zie de juridische bijlage bij dit toezichtsrapport, paragraaf II.3). Indien ook opgeslagen communicatie onder de bescherming van artikel 13 Gw komt te vallen, zal ook bij kennisname daarvan inbreuk worden gemaakt op het telecommunicatiegeheim. Hierdoor zal voor een aanzienlijk deel van de hackactiviteiten van de diensten voldaan moeten zijn aan de vereisten die de Grondwet aan een dergelijke inbreuk zal stellen.

3.5.4 Het motiveren van het verzoek om toestemming door de MIVD

De verwervende afdeling van de MIVD heeft aan de Commissie aangegeven dat het in voorkomende gevallen niet mogelijk is om de toestemmingsverzoeken voor het hacken toe te spitsen op bepaalde personen. De uitleg die hiervoor werd gegeven is dat de informatie waarover de MIVD beschikt vaak ziet op een bepaalde dreiging, zonder dat de identiteit van de personen die daarbij betrokken zijn op dat moment bekend is. In de praktijk worden verzoeken om toestemming door de verwervende afdeling gemotiveerd aan de hand van informatie die over de digitale activiteiten behorend bij een bepaald technisch kenmerk bekend is. De Commissie wijst erop dat de wet in het geval van een telefoontap de mogelijkheid biedt dat de toestemming door de minister wordt verleend onder voorwaarde

[42] Met de term 'stromende informatie' of 'stromende telecommunicatie' wordt gedoeld op telecommunicatie die *real time* wordt verworven en die daardoor op het moment van verwerving onderweg is van verzender naar ontvanger, zoals bij een telefoontap ingevolge artikel 25 Wiv 2002.

dat de ontbrekende gegevens betreffende de identiteit van de persoon of organisatie op wie de tap is gericht worden aangevuld. Zij is van oordeel dat als de MIVD beschikt over betrouwbare informatie waaruit blijkt dat bepaalde digitale activiteiten samenhangen met activiteiten die een dreiging opleveren, de persoon die deze digitale activiteiten uitvoert aangemerkt kan worden als een rechtmatig onderzoekssubject, ongeacht zijn of haar identiteit. Er is daardoor geen sprake van onrechtmatigheid. De Commissie beveelt aan dat de MIVD de gegevens betreffende de identiteit van de gebruiker(s) van het technische kenmerk indien deze bekend wordt onverwijld aanvult op de reeds gegeven motivering en ter kennis van de minister brengt.

Dit onderwerp wordt uitgebreider besproken in de geheime bijlage betreffende de MIVD bij dit toezichtsrapport.

3.5.5 Het hacken van webfora door de AIVD

Wanneer de AIVD een webforum hackt betekent dit dat het gehele forum door de dienst wordt verworven. Dit onderwerp wordt uitgebreider toegelicht in de geheime bijlage betreffende de AIVD bij dit toezichtsrapport. Onderstaand worden de bevindingen van de Commissie weergeven voor zover dit mogelijk is zonder afbreuk te doen aan de geheimhouding van bronnen, actueel kennisniveau en/of de werkwijze van de AIVD.

De Commissie constateert dat het verwerven van een geheel webforum ziet op het verwerven van een verzameling (persoons)gegevens, waaronder inhoudelijke communicatie. Het gaat hierbij om opgeslagen telecommunicatie en niet om stromende telecommunicatie in de zin van artikel 13 Gw. Bij het verwerven van een geheel webforum wordt een zware inbreuk gemaakt op de persoonlijke levenssfeer van de personen die actief zijn op dit forum. Dit feit dient naar het oordeel van de Commissie een centrale plaats te krijgen in de motivering van het verzoek om toestemming om de server waarop het desbetreffende forum is opgeslagen te hacken.

Onder de webfora die de AIVD verwerft dan wel verworven heeft, bevinden zich fora die enkel gegevens bevatten van 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 gewichtige belangen van de staat. De Commissie overweegt dat ten aanzien van dergelijke webfora in het algemeen gesteld kan worden dat de verwerving van persoonsgegevens, waaronder de inhoud van communicatie, in beginsel onder de taakuitvoering van de AIVD valt en al snel voldoet aan de vereisten van noodzakelijkheid, proportionaliteit en subsidiariteit.

Daarentegen heeft de AIVD ook webfora verworven die, naast de gegevens van (potentiële) onderzoekssubjecten van de dienst, ook de gegevens bevatten van personen die niet als zodanig zijn aan te merken. De verwerving van deze webfora kan weliswaar noodzakelijk zijn in het kader van de taakuitvoering, maar er dienen zwaarwegende operationele belangen aanwezig te zijn, wil het proportioneel zijn om de inhoudelijke communicatie te verwerven van personen die daartoe vanuit het perspectief van de nationale veiligheid geen aanleiding geven.

De rechtmatigheid van het hacken van webfora in concrete gevallen wordt beoordeeld in het onderzoek dat de Commissie thans uitvoert naar de onderzoeksactiviteiten van de AIVD op

sociale media. Het toezichtsrapport betreffende dit onderzoek zal naar verwachting begin april 2014 worden voorgelegd aan de minister.

De Commissie wijst erop dat slechts waar webfora worden verworven door middel van de hackbevoegdheid, er een separaat verzoek om toestemming van de directeur van de eenheid aanwezig is, gericht op de verwerving van het desbetreffende webforum. Daarnaast verkrijgt de AIVD echter webfora van buitenlandse diensten. In die gevallen wordt geen gemotiveerde afweging vastgelegd waarom het gerechtvaardigd is kennis te nemen van de inhoud van het webforum. De Commissie beveelt aan dat de AIVD bij de verwerving van webfora in alle gevallen ten behoeve van de (interne) toestemming afweegt in hoeverre het kennis nemen van de inhoud van het desbetreffende webforum voldoet aan het noodzakelijkheids-, proportionaliteits- en subsidiariteitsvereiste. Deze afweging dient bovendien schriftelijk te worden vastgelegd.

3.5.6 De uitvoering van de hack

Het is de Commissie gebleken dat de verwervende afdeling van de AIVD bij de uitvoering van een hack in bepaalde gevallen test of de inloggegevens (inlognaam en wachtwoord) inderdaad toegang verschaffen tot een e-mailaccount, zonder dat toestemming voor het hacken van de e-mailaccount is verleend. Hierover heeft de verwervende afdeling met de juridische afdeling afgesproken dat alleen bekeken mag worden of de inloggegevens werken. Ook de MIVD voert voorafgaand aan het opstellen van een verzoek om toestemming een vooronderzoek uit, waarin wordt onderzocht of met de bekende inloggegevens toegang kan worden verkregen tot de desbetreffende account. De Commissie constateert dat de daadwerkelijke verwerving van de inhoud van het e-mailaccount pas plaatsvindt wanneer daarvoor intern (AIVD) dan wel door de minister (MIVD) toestemming is verleend. Dit betekent dat de inhoud van het e-mailaccount niet eerder beschikbaar komt voor gebruik in het operationele proces. Met het oog op deze waarborg acht de Commissie deze werkwijze rechtmatig.

3.6 Telefonieverkeersgegevens en gebruikersgegevens

3.6.1 Algemeen

De Wiv 2002 voorziet in de bevoegdheid van de diensten om verkeersgegevens op te vragen bij telecomproviders. Tegenover de bevoegdheid deze gegevens op te vragen staat de wettelijke verplichting voor telecomproviders om aan de verzoeken van de diensten uitvoering te geven. Onder een dergelijk verzoek gegevens vallen betreffende de gebruiker (naam, adres, woonplaats, nummer), betreffende de personen of organisaties met wie de gebruiker verbinding heeft (gehad) of heeft getracht tot stand te brengen ofwel die hebben getracht verbinding met de gebruiker tot stand te brengen (naam, adres, woonplaats, telefoonnummer), gegevens betreffende de verbinding zelf (starttijd, eindtijd, locatiegegevens randapparatuur, nummers randapparatuur) en gegevens betreffende het abonnement (de soort dienst waarvan de gebruiker gebruik maakt of heeft gemaakt, de gegevens van degene die de rekening betaalt). Kort gezegd kan het bij een verzoek gaan om een combinatie van gebruikersgegevens en metagegevens. In de praktijk worden met behulp van een dergelijk verzoek door de AIVD alleen metagegevens verkregen. Deze gegevens kunnen worden opgevraagd over een bepaalde periode in het verleden, maar het is ook mogelijk dat de gegevens *real time* worden opgevraagd (zie de juridische bijlage bij dit toezichtsrapport, paragraaf V.2.6).

Artikel 29 Wiv 2002 heeft betrekking op een deel van de gegevens die op basis van artikel 28 Wiv 2002 kunnen worden opgevraagd: de gebruikersgegevens, ook wel abonneegegevens genoemd. Het gaat om naam, adres, woonplaats, nummer en soort dienst van een gebruiker. Deze gegevens worden niet opgevraagd bij de afzonderlijke telecomproviders, maar bij het CIOT (zie de juridische bijlage bij dit toezichtsrapport, paragraaf V.2.7).

3.6.2 De toestemming voor het opvragen van telefonieverkeersgegevens of gebruikersgegevens

Voor de inzet van de bijzondere bevoegdheden met betrekking tot het opvragen van verkeers- en gebruikersgegevens is niet vereist dat een *schriftelijke* motivering van de noodzakelijkheid, proportionaliteit en subsidiariteit wordt opgesteld. De Commissie heeft echter in het verleden aanbevolen – in een toezichtsrapport dat betrekking had op de MIVD – dat zij het vastleggen van de motivering voor de inzet van deze bevoegdheden ten behoeve van de interne en externe controle alsmede uit oogpunt van de zorgvuldigheid van belang acht.[43]

Het is de Commissie gebleken dat beide diensten, ondanks het ontbreken van een wettelijke plicht daartoe, thans voorzien in een schriftelijke motivering van de noodzakelijkheid, proportionaliteit en subsidiariteit van verzoeken om de inzet van artikelen 28 of 29 Wiv 2002. Dit geschiedt in het kader van het intern vragen van toestemming voor de inzet van de bevoegdheid door het desbetreffende operationele team of bureau. De Commissie constateert dat deze verzoeken om toestemming gericht zijn op een bepaald onderzoekssubject (persoon of organisatie). Er is in dit kader geen sprake van het ongericht opvragen van (verzamelingen) telefonieverkeersgegevens en/of gebruikersgegevens.

Het opvragen van telefonieverkeersgegevens dient door het hoofd van de desbetreffende dienst te geschieden. Dit is naar het oordeel van de Commissie ook het wettelijke vereiste toestemmingsniveau voor de inzet van deze bevoegdheid. Ten aanzien van het opvragen van gebruikersgegevens staat de wet toe dat het hoofd van de dienst deze bevoegdheid mandateert. Binnen de AIVD geldt dat het teamhoofd van het desbetreffende operationele team om toestemming dient te worden gevraagd. Binnen de MIVD is deze bevoegdheid belegd bij het hoofd van de verwervende afdeling. Een verschil tussen de diensten wat betreft de procedures voor het aanvragen van de toestemming voor de inzet van artikel 28 of artikel 29 Wiv 2002 is dat de aanvraag binnen de MIVD wordt gecontroleerd en geautoriseerd door de juridische afdeling voordat het aan de dienstleiding dan wel hoofd van de verwervende afdeling wordt voorgelegd, terwijl er binnen de AIVD geen juridische toets plaatsvindt.

Wanneer de diensten een telefoonnummer onderkennen waarvan het voor een onderzoek in het kader van hun inlichtingen- en/of veiligheidstaken van belang is de identiteit van de gebruiker te achterhalen, wordt ten eerste bezien of het nummer reeds bekend is binnen de dienst en welke informatie beschikbaar is over de gebruiker. Indien binnen de dienst niet de benodigde informatie beschikbaar is, kan worden overgegaan tot het vragen van toestemming voor het opvragen van de gebruikersgegevens. De gegevens van de gebruiker van het nummer worden dan opgevraagd bij het CIOT. Een andere mogelijkheid is dat tegelijk telefonieverkeersgegevens en gebruikersgegevens worden opgevraagd bij de desbetreffende telecomprovider op basis van artikel 28 Wiv 2002. In een dergelijk geval dient

[43] Toezichtsrapport van de CTIVD nr. 25 inzake het handelen van de MIVD jegens twee geschorste medewerkers, *Kamerstukken II* 2009/10, 29 924, nr. 59 (bijlage), www.ctivd.nl, paragraaf 4.2.

het op basis van de beschikbare informatie al duidelijk te zijn dat het in het kader van het onderzoek noodzakelijk is zicht te krijgen op het netwerk van de desbetreffende persoon.

3.6.3 Het verzoek aan het CIOT

Het bevragen van het CIOT gebeurt bij beide diensten geautomatiseerd. Een naslag mag pas plaatsvinden indien er toestemming op het juiste niveau is verkregen. Dit wordt door de beide diensten op verschillende wijzen gewaarborgd. Bij de AIVD dient de medewerker van het operationele team het verzoek in bij het telecomloket van de verwervende afdeling. Dit loket controleert of een last aanwezig is voor de aanvraag en verricht vervolgens door middel van een applicatie de naslag. Het resultaat wordt doorgezet naar het team. De MIVD beschikt over een beperkt aantal accounts voor het geautomatiseerd bevragen van het CIOT die worden gebruikt door medewerkers van de operationele bureaus. Het kenmerk van de artikel 29-last die is verkregen dient ingevoerd te worden bij iedere naslag, zodat altijd duidelijk is aan welke last de naslag is gekoppeld. Door het beperkte aantal accounts en door het invoeren van het nummer van de last is het altijd traceerbaar welke medewerker de naslag heeft uitgevoerd.

3.6.4 Het verstrekken van telefonieverkeersgegevens door de MIVD aan de AIVD

Het is de Commissie gebleken dat de MIVD de lijsten met telefonieverkeersgegevens die de dienst van telecomproviders ontvangt naar aanleiding van verzoeken ingevolge de Wiv 2002 standaard deelt met de AIVD. De reden hiervoor is dat de AIVD vanwege zijn taakstelling meer informatie heeft dan de MIVD op het gebied van contraterrorisme en daardoor beter in staat is de betrokkene en de telefoonnummers in de lijst te beoordelen op relevantie in dit kader. De AIVD verstrekt in voorkomende gevallen een samenvatting van de informatie die beschikbaar is aan de MIVD.

De Commissie overweegt dat de diensten de wettelijke plicht hebben elkaar zoveel mogelijk medewerking te verlenen en dat deze medewerking in ieder geval kan bestaan uit de verstrekking van gegevens. Artikel 58 Wiv 2002 vormt dan ook de wettelijke basis voor de verstrekking van gegevens tussen de diensten. Zoals iedere vorm van gegevensverwerking dient gegevensverstrekking noodzakelijk te zijn voor een goede uitvoering van de Wiv 2002 en dient het bovendien behoorlijk en zorgvuldig te zijn. De Commissie is van oordeel dat bij de beschreven werkwijze voldaan wordt aan deze vereisten, omdat nadere duiding van de verkregen informatie noodzakelijk kan worden geacht voor het onderzoek van de MIVD en het in het kader van dit doel niet onevenredig te achten is[44] dat de diensten in voorkomende gevallen over en weer gebruik maken van informatie die de andere dienst reeds in het kader van diens taakuitvoering heeft verworven. Wat betreft het vereiste dat gegevensverwerking zorgvuldig dient te zijn merkt de Commissie op dat zij geen aanwijzingen heeft dat de MIVD niet zorgvuldig handelt bij het verstrekken van telefonieverkeersgegevens aan de AIVD.

[44] De evenredigheid van het gekozen middel ten opzichte van het doel vormt een onderdeel van de vereiste zorgvuldigheid.

4 Het gebruik van gegevens op het gebied van telecommunicatie door de AIVD en de MIVD

4.1 De opslag en de ontsluiting van gegevens op het gebied van telecommunicatie

De gegevens die de diensten verwerven op het gebied van telecommunicatie vanuit de inzet van hun algemene en bijzondere bevoegdheden (zie de juridische bijlage bij dit toezichtsrapport, paragraaf V) zijn bedoeld om te benutten in het operationele proces en te combineren met andere gegevens teneinde rapportages op te stellen. Hiertoe worden de gegevens na verkrijging digitaal opgeslagen op servers en ontsloten via computerprogramma's (applicaties).

Beide diensten gebruiken voor de ontsluiting van gegevens die uit bijzondere bevoegdheden zijn verkregen (bijvoorbeeld de audiobestanden van een telefoontap of de gegevens uit een gehackt e-mailaccount) in de meeste gevallen applicaties waarbij de op grond van de Wiv 2002 en eventueel het desbetreffende mandaatbesluit vereiste toestemming voor de inzet van de bevoegdheid als het ware de toegangspoort vormt tot de gegevens. Dit betekent dat alleen de medewerkers die toestemming voor de inzet van de bevoegdheid hebben aangevraagd en eventueel medewerkers die betrokken zijn bij het uitwerken dan wel vertalen van gesprekken, berichten of andere informatie toegang hebben tot de gegevens. Daarnaast hebben de medewerkers die belast zijn met het functioneel of het technisch beheer van de applicatie toegang tot de ruwe gegevens.

De bovenstaande beschrijving kan worden aangemerkt als de algemene werkwijze bij het ontsluiten van gegevens die uit bijzondere bevoegdheden zijn verkregen. De Commissie is van oordeel dat deze werkwijze aansluit bij de wettelijke vereisten op het gebied van de interne toegang tot gegevens die - kort gezegd - inhouden dat medewerkers van de diensten alleen toegang mogen krijgen tot gegevens voor zover dat noodzakelijk is voor een goede uitvoering van hun taak en dat de hoofden van de diensten zorg moeten dragen voor de nodige voorzieningen ter beveiliging tegen onbevoegde gegevensverwerking (zie de juridische bijlage bij dit toezichtsrapport, paragraaf IV.1).

Het is de Commissie gebleken dat er twee uitzonderingen bestaan op deze algemene werkwijze. Ten eerste wordt binnen de AIVD gebruikt gemaakt van applicaties waarbinnen ruwe gegevens voor analysedoeleinden worden samengevoegd en waarvan breder gebruik wordt gemaakt dan alleen ten behoeve van het onderzoek in het kader waarvan de gegevens zijn verworven. Deze samenvoeging wordt besproken in paragraaf 4.2 van dit toezichtsrapport. Ten tweede wordt de inhoud van de webfora die de AIVD heeft verworven ontsloten door middel van een applicatie die toegankelijk is voor medewerkers van meerdere operationele teams. Deze applicatie komt nader aan de orde in paragraaf 4.3 van dit toezichtsrapport.

De gegevens die door middel van bijzondere bevoegdheden zijn verworven worden na de ontsluiting daarvan door de bij het onderzoek betrokken (audio)bewerkers, analisten en eventueel linguïsten, bewerkt en geduid. Bij deze stap worden de gegevens die relevant zijn voor het desbetreffende onderzoek of eventueel voor een ander lopend onderzoek[45] gescheiden van de gegevens die daarvoor niet relevant zijn om nader te worden verwerkt. De gegevens worden vervolgens aangemerkt als geëvalueerde gegevens. Het ruwe

[45] Dit wordt omschreven als bijvangst.

materiaal, dat wil zeggen de gegevens die nog niet op relevantie zijn beoordeeld, blijft in de meeste gevallen enige tijd bewaard.

De Commissie constateert dat geen eenduidig antwoord kan worden gegeven op de vraag hoe lang ruwe gegevens mogen worden bewaard in afwachting van eventuele nadere verwerking zolang nog niet is vastgesteld of zij relevant zijn voor het onderzoek waarbinnen zij zijn verworven of voor een ander lopend onderzoek. Deze situatie dient te worden onderscheiden van de situatie waarin de AIVD of de MIVD heeft vastgesteld dat bepaalde gegevens *niet* relevant zijn voor het onderzoek waarbinnen zij zijn verworven. Hierover is de wet duidelijk: in dat geval dienen de gegevens te worden verwijderd en uiteindelijk vernietigd. De Wiv 2002 schrijft alleen bij sigint gegevens die ongericht zijn geïntercepteerd een maximale bewaarperiode voor: deze gegevens mogen voor een periode van ten hoogste een jaar worden bewaard ten behoeve van nadere selectie. Voor andere ruwe gegevens die door middel van de inzet van bijzondere bevoegdheden zijn verworven, zoals tapgegevens of gegevensverzamelingen die met een hack zijn verkregen, is geen bewaartermijn opgenomen in de Wiv 2002. De Commissie acht het in het kader van de bescherming van de persoonlijke levenssfeer van diegenen over wie de AIVD en de MIVD gegevens verwerven, van belang dat de wet nadere aanknopingspunten biedt voor de maximale bewaartermijn van ruwe gegevens in andere gevallen. Zij beveelt aan dat dit punt wordt betrokken bij de komende wijzigingen van de Wiv.

De geëvalueerde gegevens die relevant worden geacht voor het onderzoek worden zodanig opgeslagen dat zij breder toegankelijk zijn. Beide diensten beschikken over dienstbrede applicaties die het mogelijk maken om alle geëvalueerde gegevens waarvoor medewerker zijn geautoriseerd, te doorzoeken.

4.2 De analyse van gegevens op het gebied van telecommunicatie

Naast het handmatig raadplegen, samenbrengen en met elkaar in verband brengen van gegevens, beschikken beide diensten over applicaties die geautomatiseerde analyse van de gegevens mogelijk maken. De Commissie onderscheidt in de applicaties die de diensten gebruiken bij de analyse van gegevens op het gebied van telecommunicatie drie categorieën: (1) analyseapplicaties ten behoeve van naslag in geïntegreerde gegevensbronnen, (2) analyseapplicaties ten behoeve van netwerkanalyse en (3) analyseapplicaties die gebruik maken van uitgebreide visualisatie en analysetechnieken.

Een gemene deler bij deze applicaties is dat daarmee gegevens uit verschillende bronnen kunnen worden samengevoegd en geanalyseerd. Dit betekent echter niet per definitie dat de compartimentering hierbij wordt losgelaten; bij een aantal analyseapplicaties krijgen medewerkers alleen toegang tot de ruwe gegevens uit bijzondere bevoegdheden die binnen het onderzoek waar zij bij betrokken zijn, zijn ingezet. Samenvoegen houdt in dit verband in dat de ruwe opbrengst van verschillende bijzondere bevoegdheden die binnen het desbetreffende onderzoek zijn ingezet wordt samengevoegd ter analyse, soms verrijkt met andere gegevens (zoals geografisch kaartenmateriaal). Binnen de AIVD wordt gebruik gemaakt van applicaties die voor analysedoeleinden toegang verschaffen tot samengevoegde gegevens uit verschillende bronnen, waaronder ruwe gegevens uit de inzet van bijzondere bevoegdheden. Deze applicaties zijn slechts voor één van de verwervende afdelingen van de AIVD en daarbuiten voor een zeer beperkt aantal bewerkers toegankelijk.

De Commissie heeft zich afgevraagd hoe het samenvoegen en analyseren van de ruwe opbrengst van de inzet van bijzondere bevoegdheden zich verhoudt tot de door de Wiv 2002

vereiste doelbinding en de bepalingen ten aanzien van de inzet van bijzondere bevoegdheden (zie de juridische bijlage bij dit toezichtsrapport, paragrafen III en IV). Gegevens die door middel van een bijzondere bevoegdheid worden verkregen, worden met een specifiek doel verworven. Dat doel dient gelegen te zijn binnen de inlichtingen- of veiligheidstaken van de diensten (artikel 18 Wiv 2002)[46] en te worden vastgelegd in de motivering van het verzoek om toestemming. Voor zover het gaat om de ruwe opbrengst van de inzet van een bijzondere bevoegdheid is echter nog niet vastgesteld of deze relevant is voor het onderzoek. De vraag dient zich dan aan of deze ruwe gegevens ook voor andere lopende onderzoeken en zelfs andere wettelijke taken van de diensten mogen worden aangewend dan waarvoor zij in eerste instantie zijn verworven. Beargumenteerd zou kunnen worden dat indien gegevens rechtmatig zijn verworven door middel van de inzet van een bijzondere bevoegdheid, deze gegevens daarna mogen worden aangewend voor alle taken van de diensten. De Commissie is evenwel van oordeel dat de bescherming van de persoonlijke levenssfeer noodzaakt tot het beperken van de inbreuk die wordt gemaakt door de inzet van een bijzondere bevoegdheid, door de ruwe opbrengst daarvan alleen aan te wenden in het kader van het onderzoek waarbinnen de gegevens zijn verworven of ten behoeve van een ander lopend onderzoek dat onder de inlichtingen- of veiligheidstaken van de diensten valt.[47] De Commissie wijst erop dat wanneer de gegevens eenmaal geëvalueerd zijn, zij vervolgens in het kader van alle taken van de diensten (dus ook andere dan de inlichtingen- en veiligheidstaken) mogen worden aangewend.

De Commissie constateert dat het bij de ruwe gegevens uit bijzondere bevoegdheden die door de AIVD worden samengevoegd om door middel van applicaties te worden geanalyseerd gaat om metagegevens (zie ook paragraaf 3.3.3 van dit toezichtsrapport). Voor zover deze analyse plaatsvindt in het kader van lopende onderzoeken die onder de inlichtingen- of veiligheidstaken van de AIVD vallen, is de Commissie van oordeel dat het gebruik van de samengevoegde metagegevens rechtmatig is. Dit betekent dat deze metagegevens niet mogen worden aangewend voor andere andere dan de inlichtingen- en veiligheidstaken van de dienst.

4.3 Het gebruik van gegevens uit webfora door de AIVD

De AIVD maakt bij het verwerken van de gegevens uit webfora gebruik van een applicatie waarin de webfora waar de dienst over beschikt zijn opgenomen. Deze applicatie is bedoeld voor zowel de ontsluiting van de gegevens als de analyse daarvan. Dit heeft te maken met het feit dat webfora teveel gegevens bevatten om deze integraal door te nemen zoals gebeurt bij de audiobestanden van een telefoontap. Dit onderwerp wordt uitgebreider besproken in de geheime bijlage betreffende de AIVD bij dit toezichtsrapport. Onderstaand worden de bevindingen van de Commissie in algemene bewoordingen weergegeven, zonder afbreuk te doen aan de geheimhouding van bronnen, actueel kennisniveau en/of de werkwijze van de AIVD.

---

[46] Artikel 18 bepaalt dat bijzondere bevoegdheden alleen mogen worden ingezet voor zover dat noodzakelijk is voor de goede uitvoering van de a- en de d-taken van de AIVD en de a-, c- en e-taken van de MIVD. De wet staat derhalve niet toe dat bijzondere bevoegdheden worden ingezet in het kader van veiligheidsonderzoeken (de b-taak van de diensten), in het kader van veiligheidsbevordering (de c-taak van de AIVD, de d-taak van de MIVD) of in het kader van het stelsel bewaken en beveiligen (de e-taak van de AIVD, de f-taak van de MIVD).

[47] In dergelijke gevallen wordt gesproken van bijvangst.

De applicatie voor het verwerken van webfora is toegankelijk voor bepaalde medewerkers van operationele teams. De desbetreffende medewerker dient vervolgens ook geautoriseerd te zijn voor toegang tot een specifiek forum. Deze autorisatie wordt gegeven op basis van relevantie voor de onderzoeken waar de medewerker bij betrokken is. De Commissie constateert dat deze werkwijze in overeenstemming is met het vereiste dat verstrekking van gegevens binnen de dienst slechts plaatsvindt voor zover dat noodzakelijk is voor een goede uitvoering van de aan de desbetreffende ambtenaar opgedragen taak (artikel 35 Wiv 2002). Zij wijst erop dat de ruwe (ongeëvalueerde) gegevens in de applicatie slechts mogen worden gebruikt voor lopende onderzoeken die vallen onder de inlichtingen- of veiligheidstaak van de dienst.

In het onderzoek van de Commissie is naar voren gekomen dat de webfora die door middel van de applicatie worden ontsloten doorgaans beschikbaar blijven. De AIVD heeft aangegeven dat de relevantie van de verworven webfora altijd blijft bestaan, omdat de gegevens benodigd zijn voor bepaalde operationele doelen. De Commissie merkt op dat zij het bewaren en beschikbaar houden van gehele webfora, zeker waar het gaat om fora waarvan niet iedere deelnemer op voorhand als (potentieel) onderzoekssubject van de AIVD kan worden aangemerkt ziet als een zwaar middel dat in verhouding dient te staan tot het operationele doel daarvan (zie tevens paragraaf 3.5.5. van dit toezichtsrapport). De rechtmatigheid van het bewaren van webfora wordt in concrete gevallen beoordeeld in het onderzoek dat de Commissie thans uitvoert naar de onderzoeksactiviteiten van de AIVD op sociale media. Het toezichtsrapport betreffende dit onderzoek zal naar verwachting begin april 2014 worden voorgelegd aan de minister.

5 De uitwisseling van gegevens op het gebied van telecommunicatie met buitenlandse inlichtingen- en veiligheidsdiensten door de AIVD en de MIVD

5.1 Samenwerkingsrelaties met buitenlandse inlichtingen- en veiligheidsdiensten

De grondslag voor de samenwerking met buitenlandse inlichtingen- en veiligheidsdiensten ligt allereerst besloten in de Wiv 2002, waarin is bepaald dat de hoofden van de diensten verbindingen onderhouden met daarvoor in aanmerking komende buitenlandse diensten. Of een buitenlandse dienst *in aanmerking komt* voor hechte samenwerking dient door de Nederlandse diensten te worden afgewogen aan de hand van een aantal criteria, waaronder de mate van respect voor de mensenrechten, democratische inbedding en professionaliteit en betrouwbaarheid.[48] De samenwerking met buitenlandse diensten is daarnaast gebaseerd op een zekere mate van wederzijds vertrouwen en wordt nader ingevuld door afspraken die in bi- en multilateraal verband zijn gemaakt.

De Commissie heeft, naar aanleiding van de vragen die in de media en in de politiek naar voren zijn gekomen, onderzoek gedaan naar de samenwerking met buitenlandse diensten. Zij heeft haar onderzoek toegespitst op het verstrekken en ontvangen van verzamelingen (ruwe) gegevens op het gebied van telecommunicatie. In termen van de Wiv 2002 kan dit worden aangemerkt als gegevensuitwisseling of ondersteuning. In de juridische bijlage bij dit toezichtsrapport, paragrafen VI.2 t/m VI.4, wordt beschreven waar deze vormen van samenwerking conform de Wiv 2002 aan moeten voldoen.

[48] Toezichtsrapport van de CTIVD nr. 22a inzake de samenwerking van de AIVD met buitenlandse inlichtingen- en/of veiligheidsdiensten, *Kamerstukken II* 2009/10, 29 924, nr. 39 (bijlage), beschikbaar op www.ctivd.nl, paragraaf 5.

Voor zover sprake is van uitwisseling van verzamelingen (ruwe) gegevens, betreft dit een verregaande vorm van samenwerking. De Commissie constateert dat dergelijke uitwisselingen plaatsvinden binnen hechte samenwerkingsrelaties tussen bevriende landen die zijn gebaseerd op een grote mate van wederzijds vertrouwen. Deze buitenlandse diensten voldoen volgens de afwegingen van de AIVD en de MIVD aan de criteria voor samenwerking. Het wederzijdse vertrouwen is niet onbegrensd. Concrete voorvallen of mediaberichten zijn in het verleden reeds aanleiding geweest om de samenwerking met sommige van deze diensten op bepaalde punten te heroverwegen. Ook dienen de AIVD en de MIVD zich er rekenschap van te geven dat de Nederlandse belangen die zij behartigen niet te allen tijde parallel lopen aan de belangen van die buitenlandse diensten en omgekeerd. De Commissie constateert dat voor wat betreft de onderzochte samenwerkingsrelaties op het vlak van de uitwisseling van (ruwe) gegevens, er telkens een duidelijk gezamenlijk belang aanwezig is, zoals in het kader van de strijd tegen het terrorisme en van militaire operaties in het buitenland.

De Commissie wijst erop, in navolging van de opmerkingen daaromtrent in de Kamerstukken bij de Wiv 2002, dat het in het algemeen in het internationaal verkeer tussen inlichtingen- en veiligheidsdiensten niet gebruikelijk is om bij de buitenlandse dienst te informeren naar de bron of de methode die gebruikt is om gegevens te vergaren, noch om zelf informatie te verstrekken over de wijze waarop gegevens zijn verworven.[49] De wetgever achtte het evenwel niet ondenkbaar dat in sommige vertrouwde relaties of ten behoeve van gezamenlijke operaties meer openheid wordt betracht ten aanzien van de bronnen van de diensten.[50]

De Commissie constateert dat de AIVD en de MIVD in de onderzochte hechte samenwerkingsverbanden er in grote mate op vertrouwen dat de desbetreffende buitenlandse diensten mensenrechten respecteren en handelen binnen de eigen nationale regelgeving. De Commissie is van mening dat het in het licht van de onthullingen van de afgelopen periode gewenst is om na te gaan of dit vertrouwen nog steeds terecht is. Voortvloeiend uit de wet[51] is het aan de hoofden van de AIVD en de MIVD onder de politieke verantwoordelijkheid van de betrokken minister te overwegen of buitenlandse diensten nog steeds in aanmerking komen voor de verschillende vormen van samenwerking die plaatsvinden in het kader van de hechte samenwerkingsrelatie.[52] Concreet betekent dit dat zij zich nader dienen te informeren over de wettelijke bevoegdheden en (technische) mogelijkheden van buitenlandse diensten, opdat zij verantwoorde afwegingen kunnen maken. De Commissie beveelt de ministers van BZK en van Defensie in dit verband tevens aan de samenwerkingsrelaties (ook in internationaal verband) te beoordelen op transparantie en de afwegingen die ten grondslag liggen aan de samenwerking nader te concretiseren.

Samenwerking met buitenlandse diensten vindt in het algemeen plaats volgens het *quid pro quo* of wederkerigheidsbeginsel. Het uitgangspunt is kort gezegd: 'voor wat, hoort wat', en

---

[49] *Kamerstukken II* 2000/01, 25 877, nr. 14, p. 63.

[50] *Kamerstukken II* 2000/01, 25 877, nr. 14, p. 63.

[51] In artikel 59 Wiv 2002 is de zorgplicht van de hoofden van de AIVD en de MIVD neergelegd voor het onderhouden van verbindingen met daarvoor in aanmerking komende buitenlandse diensten.

[52] Toezichtsrapport van de CTIVD nr. 22a inzake de samenwerking van de AIVD met buitenlandse inlichtingen- en/of veiligheidsdiensten, *Kamerstukken II* 2009/10, 29 924, nr. 39 (bijlage), beschikbaar op www.ctivd.nl, paragraaf 5.1 en 6.1.

vormt een stelregel in de inlichtingen- en veiligheidswereld.[53] Indien de AIVD en de MIVD gegevens *verstrekken* of ondersteuning *verlenen*, dan gelden hiervoor de normen voor het verstrekken van (persoons)gegevens en de inzet van bijzondere bevoegdheden zoals de Wiv 2002 deze stelt.[54] In de paragrafen 5.4 - 5.6 toetst de Commissie ten aanzien van enkele bestaande hechte samenwerkingsverbanden in hoeverre de verstrekking van verzamelingen (ruwe)gegevens en ondersteuning door de AIVD en de MIVD rechtmatig heeft plaatsgevonden. Indien de AIVD en de MIVD gegevens of ondersteuning *ontvangen*, dan is de juridische toets die zij op basis van de Wiv 2002 moeten verrichten beperkter. De Commissie bespreekt dit in paragraaf 5.2.

In de paragrafen 5.4 – 5.6 wordt in algemene bewoordingen ingegaan op enkele samenwerkingsrelaties, zonder afbreuk te doen aan de geheimhouding van bronnen, actueel kennisniveau en/of de werkwijze van de diensten. In de geheime bijlagen bij dit toezichtsrapport heeft de Commissie haar bevindingen nader uiteen gezet ten aanzien van een aantal (categorieën) samenwerkingsrelaties. De Commissie wijst erop dat in dit toezichtsrapport en in de geheime bijlagen niet wordt beoogd een uitputtend overzicht te geven van de bestaande hechte samenwerkingsrelaties.

5.2 Het door de AIVD en de MIVD ontvangen van gegevens en ondersteuning

Als ontvanger van gegevens of ondersteuning hebben de AIVD en de MIVD op basis van de Wiv 2002 een beperkte juridische taak. In de Kamerstukken bij de wet wordt gesteld dat de verantwoordelijkheid voor de rechtmatigheid van de gegevensverzameling in dit kader ligt bij de verstrekkende buitenlandse dienst.[55] De buitenlandse dienst wordt geacht zich aan de eigen wettelijke kaders te houden. De AIVD en de MIVD mogen er dan ook, zonder concrete aanwijzingen voor het tegendeel, van uitgaan dat die wet- en regelgeving in acht is genomen. In hechte samenwerkingsrelaties betekent dit, dat de AIVD en de MIVD reeds in het algemeen hebben vastgesteld dat deze buitenlandse diensten voldoen aan de criteria voor samenwerking, waaronder de democratische inbedding en het respect voor de mensenrechten. De AIVD en de MIVD moeten zich op hun beurt aan de Nederlandse wet houden wanneer zij een buitenlandse dienst *verzoeken* om informatie of ondersteuning, of wanneer zij ontvangen informatie willen *gebruiken*. Dit betekent dat voorafgaande aan een verzoek om bepaalde gegevens of ondersteuning zij een afweging moeten maken in hoeverre de gewenste gegevensverstrekking of ondersteuning voldoet aan de vereisten van noodzakelijkheid, proportionaliteit en subsidiariteit. Het is de AIVD en de MIVD niet toegestaan een buitenlandse dienst te verzoeken een bevoegdheid in te zetten waar de Nederlandse diensten zelf niet over beschikken (de U-bochtconstructie). De diensten moeten zich daarnaast onthouden van het gebruik van gegevens waarvan bekend is of vermoed wordt dat zij door de buitenlandse dienst zijn verworven met gebruik van een methode die een ongeoorloofde inbreuk op enig grondrecht maakt (zie de juridische bijlage bij dit toezichtsrapport, paragrafen VI.3 en VI.4).

De Commissie signaleert dat sommige buitenlandse diensten, anders dan de AIVD en de MIVD, de bevoegdheid hebben om ongericht kabelgebonden telecommunicatie te

---

[53] Toezichtsrapport van de CTIVD nr. 22a inzake de samenwerking van de AIVD met buitenlandse inlichtingen- en/of veiligheidsdiensten, *Kamerstukken II* 2009/10, 29 924, nr. 39 (bijlage), beschikbaar op www.ctivd.nl, paragraaf 5.5.
[54] *Kamerstukken II* 2000/01, 25 877, nr. 14, p. 62, zie ook de juridische bijlage bij dit toezichtsrapport, paragrafen VI.2 enVI.4
[55] *Kamerstukken II* 2000/01, 25 877, nr. 14, p. 62.

intercepteren. Dit valt voor hen onder het begrip sigint. De vraag die hierbij rijst is of de AIVD en de MIVD, als zij met deze diensten samenwerken op het terrein van sigint, gebruik maken van een zogenaamde U-bochtconstructie. Zij kunnen zo immers toegang verkrijgen tot gegevens die worden verzameld met de inzet van een bevoegdheid waar zij zelf niet over beschikken. Enerzijds is het van belang dat het de AIVD en de MIVD bekend kan zijn dat zij in het kader van deze samenwerking ook gegevens ontvangen die afkomstig zijn uit ongerichte kabelgebonden interceptie. Dit is op voorhand immers niet uitgesloten. Anderzijds is het van belang dat de AIVD en de MIVD hier niet expliciet om verzoeken, maar het de verstrekkende buitenlandse dienst is die een brede definitie van sigint hanteert. De Commissie geeft hierbij in overweging dat het feit dat de Wiv 2002 niet voorziet in de bevoegdheid ongericht kabelgebonden telecommunicatie te intercepteren niet betekent dat dergelijke interceptie op zichzelf reeds een ongeoorloofde inbreuk op de persoonlijke levenssfeer oplevert. Aan de AIVD en de MIVD is immers in de Wiv 2002 een vergelijkbare bevoegdheid toegekend ten aanzien van niet-kabelgebonden telecommunicatie. Bij de totstandkoming van de Wiv 2002 is geen expliciete grondrechtelijke afweging gemaakt over het verschil tussen kabelgebonden en niet-kabelgebonden telecommunicatie. Ook kan niet op voorhand worden gezegd dat kabelgebonden interceptie, indien voorzien van dezelfde waarborgen die gelden voor niet-kabelgebonden interceptie, op zichzelf in strijd is met het EVRM of andere mensenrechtenverdragen. De Commissie acht het in dit verband toegestaan dat de AIVD en de MIVD samenwerken met deze buitenlandse diensten, ook als niet uitgesloten kan worden dat zij gegevens ontvangen die zijn verkregen door ongerichte interceptie van kabelgebonden telecommunicatie.

De Commissie heeft in haar onderzoek geen aanwijzingen gevonden dat de AIVD en de MIVD expliciet verzoeken hebben gericht aan buitenlandse diensten om methoden in te zetten die naar Nederlands recht niet geoorloofd zijn.

5.3 Activiteiten van buitenlandse diensten op Nederlands grondgebied

In Nederland hebben buitenlandse inlichtingen- en/of veiligheidsdiensten de toestemming van de minister van BZK nodig om op Nederlands grondgebied inlichtingenactiviteiten te mogen ontplooien. Voor zover het gaat om activiteiten op plaatsen in gebruik bij het ministerie van Defensie is dit de minister van Defensie. In de wetsgeschiedenis is benadrukt dat de Wiv 2002 exclusief regelt dat uitsluitend de AIVD en de MIVD in Nederland bevoegd zijn en onder welke voorwaarden die bevoegdheid uitgeoefend mag worden. Dit betekent dat het is uitgesloten dat een buitenlandse inlichtingen- en veiligheidsdienst wordt toegestaan zelfstandig en naar eigen inzichten in Nederland inlichtingenactiviteiten te ontplooien.[56]

Wordt toestemming verleend voor activiteiten van buitenlandse diensten op Nederlands grondgebied, dan geschiedt dit onder verantwoordelijkheid van de minister en onder leiding van de Nederlandse dienst. Een dergelijke operatie is altijd aan te merken als een gezamenlijke operatie waarbij de buitenlandse dienst als gelijkwaardige partner optreedt. Het is voorts aan de Nederlandse dienst om controle uit te oefenen op het opereren van de buitenlandse collega en om na te gaan of dit opereren aan de gestelde voorwaarden voldoet.[57]

---

[56] *Kamerstukken I* 2001/02, 25 577, nr. 58a, p. 25.
[57] *Kamerstukken II* 2000/01, 25 877, nr. 14, p. 64.

De Commissie heeft bij haar onderzoek uitdrukkelijk de samenwerkingsverbanden op het gebied van sigint en cyber betrokken. Zij heeft daarbij geen aanwijzingen gevonden dat buitenlandse diensten met medewerking van de AIVD of de MIVD zelfstandige toegang hebben verkregen tot Nederlandse telefoon- of internetverbindingen.

5.4 Het verstrekken van metagegevens door de AIVD en de MIVD ten aanzien van bepaalde onderwerpen

Binnen een bepaald internationaal samenwerkingsverband waaraan de AIVD en de MIVD deelnemen worden door de deelnemende diensten structureel (ruwe) metagegevens uit ongerichte interceptie gedeeld betreffende onderwerpen die in gezamenlijk verband zijn afgesproken.

Het is de Commissie gebleken dat de MIVD alle Nederlandse nummers uit de lijst filtert voordat de gegevens worden gedeeld. De AIVD heeft aangegeven dit niet te doen, omdat de dienst met name IP-metagegevens verwerft en deelt en bij deze metagegevens niet met zekerheid zou zijn vast te stellen of het om een Nederlands nummer gaat.

De Commissie stelt vast dat het verstrekken van metagegevens binnen dit samenwerkingsverband geschiedt op basis van artikel 36 Wiv 2002. Ingevolge deze bepaling zijn de diensten in het kader van een goede taakuitvoering bevoegd aan daarvoor in aanmerking komende buitenlandse diensten gegevens te verstrekken. Dit betekent dat de verstrekking in dat kader noodzakelijk dient te zijn en dat voldaan dient te zijn aan de vereisten van behoorlijkheid en zorgvuldigheid (zie de juridische bijlage bij dit toezichtsrapport, paragraaf IV.1). De Commissie is van oordeel dat bij deze verstrekkingen voldaan is aan het vereiste van noodzakelijkheid in het kader van de goede taakuitvoering. Voor het beoordelen van de behoorlijkheid van de verstrekking is relevant dat het bij deze metagegevens kan gaan om persoonsgegevens en er dus sprake kan zijn van een inbreuk op de persoonlijke levenssfeer. Dit dient te worden meegewogen bij het beoordelen van de evenredigheid van het door de dienst gekozen middel ten opzichte van het doel daarvan (een onderdeel van de behoorlijkheid). In het geval van deze uitwisseling van gegevens is de Commissie van oordeel dat het doel van de verstrekking opweegt tegen de inbreuk die daardoor kan worden gemaakt op de persoonlijke levenssfeer van de betrokkenen. Het wettelijke vereiste dat gegevensverwerking zorgvuldig dient te zijn heeft in deze context onder meer betrekking op de juistheid van de gegevens die worden verstrekt en op de vastlegging van de afwegingen die aan de gegevensverstrekking ten grondslag liggen. De Commissie merkt op dat zij geen aanwijzingen heeft dat de diensten niet zorgvuldig te werk gaan.

De werkwijze van de AIVD en de MIVD bij de onderhavige structurele uitwisseling van gegevens is daarom rechtmatig naar het oordeel van de Commissie.

5.5 De inzet van de selectiebevoegdheid door de MIVD ten behoeve van partnerdiensten.

Het is de Commissie gebleken dat de MIVD binnen een internationaal samenwerkingsverband verzamelingen (ruwe) metagegevens verkregen uit ongerichte interceptie van niet-kabelgebonden telecommunicatie structureel uitwisselt met samenwerkingspartners.

De Commissie heeft zich eerder op het standpunt gesteld dat het bij de onderhavige vorm van gegevensuitwisseling niet zozeer gaat om de verstrekking van gegevens, maar om het

verlenen van technische ondersteuning in de zin van artikel 59 Wiv 2002 (zie de bijlage bij het toezichtsrapport, paragraaf VI.4).[58] Het gaat naar het oordeel van de Commissie namelijk om de inzet van een bijzondere bevoegdheid, te weten het selecteren van ongericht geïntercepteerde gegevens ten behoeve van partnerdiensten.

Het verlenen van technische ondersteuning aan een buitenlandse dienst dient te voldoen aan een aantal vereisten. Allereerst gaat het om de voorwaarden dat de belangen die de samenwerkingspartners behartigen niet onverenigbaar zijn met de belangen die de MIVD heeft te behartigen en dat een goede taakuitvoering door de MIVD zich niet tegen verstrekking verzet. De Commissie heeft geen aanwijzingen dat niet is voldaan aan deze vereisten.

Volgens de wet vindt het verlenen van ondersteuning voorts alleen plaats met toestemming van de betrokken minister. De Commissie heeft in dit geval niet vastgesteld of de minister toestemming heeft gegeven voor het verlenen van technische ondersteuning. De Commissie wijst de MIVD erop dat op enigerlei wijze dient te blijken dat de minister akkoord is gegaan met deze vorm van samenwerking, wil voldaan zijn aan het vereiste van de Wiv 2002.

Voor het waarborgen van de bescherming van de persoonlijke levenssfeer is met name essentieel dat de inzet van bijzondere bevoegdheden ter ondersteuning van een buitenlandse dienst in overeenstemming is met de Wiv 2002 en dat voldaan is aan de daarin gestelde vereisten (zie de bijlage bij dit toezichtsrapport, paragrafen VI.4 en III). Dit betekent dat bij het verlenen van ondersteuning ook aan de vereisten van noodzakelijkheid, proportionaliteit en subsidiariteit voldaan moet zijn. Het is de Commissie gebleken dat de MIVD de selectie van ongericht geïntercepteerde gegevens ten behoeve van zijn samenwerkingspartners niet aanmerkt als selectie in de zin van de wet. Om deze reden wordt ook niet per kenmerk een gemotiveerd verzoek aan de minister gericht. De Commissie is van oordeel dat de huidige werkwijze van de MIVD niet in overeenstemming is met de Wiv 2002 en geen invulling geeft aan de waarborgen die in de wet besloten liggen. Deze werkwijze is derhalve onrechtmatig. Zij beveelt aan dat de MIVD zijn werkwijze onverwijld aanpast zodat de minister voortaan op basis van een motivering aan de hand van de beschikbare informatie om toestemming wordt gevraagd voor de toepassing van de selectiebevoegdheid.

5.6 Het uitwisselen van webfora door de AIVD

De AIVD wisselt met een aantal buitenlandse diensten in bilateraal ofwel in trilateraal verband webfora uit. De Commissie constateert dat het verstrekken van een webforum ziet op het delen van een verzameling (persoons)gegevens. Het gaat om zowel inhoudelijke communicatie als metagegevens. Deze verstrekking geschiedt in het kader van de goede taakuitvoering door de AIVD op basis van de Wiv 2002. De Commissie overweegt in dit verband dat het verstrekken van webfora alleen toelaatbaar is als het noodzakelijk voor de goede taakuitvoering en behoorlijk te achten is dat de gegevens van alle betrokken personen worden verstrekt. Daarnaast dient de gegevensverstrekking te voldoen aan het vereiste van zorgvuldigheid hetgeen in deze context onder meer ziet op de juistheid van de gegevens en op de vastlegging van de afwegingen die aan de gegevensverstrekking ten grondslag liggen. Het is de Commissie gebleken dat de webfora die de AIVD heeft gedeeld in vrijwel alle gevallen webfora betreffen die enkel de gegevens bevatten van personen die door de doelen

[58] Toezichtsrapport van de CTIVD nr. 28 inzake de inzet van Sigint door de MIVD, *Kamerstukken II* 2011/12, 29 924, nr. 74 (bijlage), beschikbaar op www.ctivd.nl, paragraaf 9.3.

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 gewichtige belangen van de staat. De Commissie stelt ten aanzien van het verstrekken van dergelijke webfora in het algemeen dat dit noodzakelijk kan zijn in het kader van de goede taakuitvoering en aangemerkt kan worden als evenredig in verhouding tot het daarmee te dienen doel (een onderdeel van de behoorlijkheid). De Commissie heeft geen aanwijzingen dat bij deze verstrekkingen niet voldaan is aan het zorgvuldigheidsvereiste.

De rechtmatigheid van het verstrekken van webfora in concrete gevallen wordt thans beoordeeld in het onderzoek dat de Commissie uitvoert naar de onderzoeksactiviteiten van de AIVD op sociale media. Het toezichtsrapport betreffende dit onderzoek zal naar verwachting begin april 2014 worden voorgelegd aan de minister.

6 Conclusies en aanbevelingen

De verwerving van gegevens op het gebied van telecommunicatie door de AIVD en de MIVD

Telefoon- en internettaps (paragraaf 3.2)

De diensten zijn ingevolge artikel 25 Wiv 2002 bevoegd tot het gericht aftappen van elke vorm van telecommunicatie. Het tappen van telefoongesprekken en internetverkeer geschiedt door beide diensten op basis van lasten; toestemming van de desbetreffende minister het telefoon- of internetverkeer van- en naar een bepaald telefoonnummer of IP-adres (dan wel meerdere nummers/IP-adressen) behorend bij een bepaalde persoon of organisatie af te luisteren. De Commissie constateert dat hierbij geen sprake is van het ongericht verwerven van (verzamelingen) gegevens.

Interceptie en selectie van sigint (paragraaf 3.3)

De AIVD en de MIVD beschikken niet over de bevoegdheid kabelgebonden telecommunicatie te intercepteren. De Commissie stelt vast dat er geen ongerichte interceptie van kabelgebonden telecommunicatie plaatsvindt door de AIVD en de MIVD.

De AIVD en de MIVD zijn wel bevoegd niet-kabelgebonden communicatie ongericht te verzamelen en op te slaan (artikel 27 Wiv 2002). Het gaat hierbij zowel om de inhoud van de communicatie als om metagegevens. Slechts een deel van de inhoud van de communicatie wordt ten behoeve van kennisneming geselecteerd aan de hand van door de minister goedgekeurde selectiecriteria en gebruikt in het inlichtingenproces.

De metagegevens van de ongericht verzamelde communicatie worden nader geanalyseerd (metadata-analyse). Een deel van deze gegevens moet worden aangemerkt als persoonsgegevens. Het verwerken hiervan vormt een inbreuk op de persoonlijke levenssfeer. Het is om die reden van belang dat het proces van metadata-analyse bij wet wordt voorzien van waarborgen die beschermen tegen ongeoorloofde inbreuken op de persoonlijke levenssfeer zoals het motiveren van de noodzakelijkheid, proportionaliteit en subsidiariteit van de gegevensverwerking ten behoeve van interne dan wel externe toestemming. Dit is nu niet het geval. De Commissie beveelt aan een specifieke regeling voor de verwerking van metagegevens op te nemen in de wet.

Op basis van metadata-analyse wordt door de MIVD in de inhoud van de communicatie onderzoek gedaan naar nieuwe onderzoekssubjecten. De MIVD schaart dit onder de bevoegdheid te searchen (artikel 26 Wiv 2002). De Commissie heeft in een eerder toezichtsrapport al aangegeven dat deze werkwijze naar haar oordeel onrechtmatig is, omdat de inbreuk op de persoonlijke levenssfeer in dergelijke gevallen niet wordt ondervangen door de toestemming van de minister ten aanzien van de desbetreffende persoon of organisatie selectie te plegen. Op de werkwijze van de AIVD inzake het searchen zal worden teruggekomen in het doorlopende onderzoek van de Commissie naar de inzet van de afluisterbevoegdheid en van de bevoegdheid tot de selectie van sigint door de AIVD. Het toezichtsrapport betreffende dit onderzoek over de periode van september 2012 tot en met augustus 2013 zal naar verwachting begin april 2014 worden voorgelegd aan de minister.

De Commissie heeft in eerdere toezichtsrapporten vastgesteld dat zowel de AIVD als de MIVD de inzet van de selectiebevoegdheid onvoldoende motiveerden. Het ging hierbij om het onvoldoende toespitsen van de motivering voor de selectie op de personen en/of organisaties die in de selectielijst waren opgenomen.

Menselijke bronnen (paragraaf 3.4)

Gegevens op het gebied van telecommunicatie kunnen worden verworven met behulp van menselijke bronnen (artikel 17 of 21 Wiv 2002). De Commissie heeft geconstateerd dat door menselijke bronnen die zijn ingezet door de AIVD activiteiten zijn verricht die vergelijkbaar zijn met de bevoegdheid gesprekken, telecommunicatie en/of gegevensoverdracht af te tappen (artikel 25 Wiv 2002) en met de bevoegdheid te hacken (artikel 24 Wiv 2002). De bescherming van de persoonlijke levenssfeer vereist dat, los van de inzet van de menselijke bron, per activiteit van de bron wordt beoordeeld wat de aard daarvan is en welk type gegevens wordt verworven. Dit onder meer om te bepalen of sprake is van de inzet van bijzondere bevoegdheden door de menselijke bron, waarvoor nadere toestemming vereist is.

De Commissie is van oordeel dat het alleen mogelijk is op adequate wijze de bescherming van de persoonlijke levenssfeer te waarborgen indien de nadruk komt te liggen op de aard van de activiteit en het type gegevens dat wordt verworven, zo onafhankelijk mogelijk van het middel waarmee de gegevens worden verworven (de inzet van de menselijke bron).

In voorkomende gevallen is tot op heden binnen de AIVD geen aparte motivering opgesteld voor activiteiten van een menselijke bron die dienen te worden aangemerkt als tappen (artikel 25 Wiv 2002) of als hacken (artikel 24 Wiv 2002). Evenmin is op het juiste niveau toestemming verleend voor deze activiteiten. De Commissie acht deze werkwijze onrechtmatig voor zover het gaat om activiteiten die vergelijkbaar zijn met tappen, omdat niet is voldaan aan het wettelijke vereiste dat de minister hiervoor om toestemming dient te worden gevraagd. De Commissie acht de werkwijze van de AIVD niet zonder meer onrechtmatig waar het activiteiten betreft die dienen te worden aangemerkt als hacken, met name omdat het vereiste toestemmingsniveau in die gevallen volgt uit het Mandaatbesluit bijzondere bevoegdheden AIVD 2009 dat intern de AIVD is vastgesteld. Of de AIVD rechtmatig heeft gehandeld dient in concrete gevallen te worden beoordeeld. Bepaald moet worden of de noodzakelijkheid, proportionaliteit en subsidiariteit in voldoende mate zijn gemotiveerd. Dit wordt nader onderzocht in het onderzoek dat de Commissie thans uitvoert naar de onderzoeksactiviteiten van de AIVD op sociale media. Het toezichtsrapport betreffende dit onderzoek zal naar verwachting begin april 2014 worden voorgelegd aan de minister.

De Commissie beveelt aan dat de AIVD onverwijld zijn werkwijze aanpast door voortaan het juiste toestemmingsniveau in acht te nemen en de inzet van bijzondere bevoegdheden door menselijke bronnen separaat van de inzet van de desbetreffende menselijke bronnen te motiveren.

Hacken (paragraaf 3.5)

De AIVD en de MIVD zijn bevoegd gegevens te verwerven door middel van het binnendringen in een geautomatiseerd werk, ofwel hacken (artikel 24 Wiv 2002). Hiervoor is ingevolge de wet geen toestemming van de minister vereist. De diensten moeten ten behoeve van interne toestemming gemotiveerd aangeven welk geautomatiseerd werk het betreft en welke informatie met het hacken wordt beoogd te worden verkregen.

De Commissie heeft geconstateerd dat de AIVD de verzoeken om toestemming voor de inzet van de hackbevoegdheid soms breed verwoordt omdat op voorhand slechts beperkt duidelijk is welke informatie bij het hacken zal worden aangetroffen. De bescherming van de persoonlijke levenssfeer vereist echter dat zo gericht mogelijk wordt gemotiveerd op welke informatie het hacken is gericht. Alleen dan kan de noodzakelijkheid, proportionaliteit en subsidiariteit van de voorgenomen inzet ten volle worden beoordeeld. Wanneer bij het hacken gegevens worden aangetroffen die niet onder de toestemming vallen maar wel relevant zijn voor het onderzoek, kan –via een spoedprocedure – alsnog toestemming worden gevraagd voor het overnemen van deze gegevens.

Bij de inzet van de hackbevoegdheid door de AIVD wordt in bepaalde gevallen kennis genomen van stromende telecommunicatie in de zin van artikel 25 Wiv 2002. Dit houdt in dat in feite sprake is van de inzet van de tapbevoegdheid door de AIVD. Voor zover geen toestemming is gevraagd van de minister in dergelijke gevallen, is de Commissie van oordeel dat het handelen terzake onrechtmatig is geweest. Zij beveelt aan dat de AIVD onverwijld zijn werkwijze in overeenstemming brengt met het wettelijke vereiste dat er toestemming dient te worden gevraagd aan de minister van BZK wanneer kennis wordt genomen van stromende telecommunicatie in de zin van artikel 25 Wiv 2002.

Voor de MIVD is het in voorkomende gevallen niet mogelijk de toestemmingsverzoeken voor het hacken toe te spitsen op bepaalde personen. De toestemmingsverzoeken worden gemotiveerd aan de hand van informatie die over de digitale activiteiten behorend bij een bepaald technisch kenmerk bekend is. De Commissie is van oordeel dat hierbij geen sprake is van onrechtmatigheid. Zij beveelt aan dat de MIVD de gegevens betreffende de identiteit van de gebruiker(s) van het technische kenmerk indien deze bekend wordt onverwijld aanvult op de reeds gegeven motivering en ter kennis van de minister brengt.

De AIVD verwerft door middel van hacken gehele webfora. Dit betreft verzamelingen persoonsgegevens, waaronder inhoudelijke communicatie. Het gaat hierbij om opgeslagen telecommunicatie en geen stromende telecommunicatie in de zin van artikel 13 Gw. Over het verwerven van webfora waarvan alle deelnemers op voorhand als (potentiële) onderzoekssubjecten van de AIVD kunnen worden aangemerkt kan in het algemeen worden gesteld dat dit in beginsel onder de taakuitvoering van de AIVD valt en al snel voldoet aan de vereisten van proportionaliteit en subsidiariteit. Dit ligt anders bij webfora die, naast de gegevens van (potentiële) onderzoekssubjecten van de dienst, ook de gegevens bevatten van personen die niet als zodanig zijn aan te merken. De verwerving van deze webfora kan weliswaar noodzakelijk zijn in het kader van de taakuitvoering, maar er dienen

zwaarwegende operationele belangen aanwezig te zijn wil het proportioneel zijn om de communicatie te verwerven van personen die daartoe vanuit het perspectief van de nationale veiligheid geen aanleiding geven. De rechtmatigheid van het hacken van webfora in concrete gevallen wordt beoordeeld in het onderzoek dat de Commissie uitvoert naar de onderzoeksactiviteiten van de AIVD op sociale media. Het toezichtsrapport betreffende dit onderzoek zal naar verwachting begin april 2014 worden voorgelegd aan de minister.

Slechts waar webfora worden verworven door middel van de hackbevoegdheid (artikel 24 Wiv 2002) is er een separaat verzoek om toestemming van de directeur van de eenheid aanwezig, gericht op de verwerving van het desbetreffende webforum. Daarnaast verkrijgt de AIVD echter webfora van buitenlandse diensten. In die gevallen wordt geen gemotiveerde afweging vastgelegd waarom het gerechtvaardigd is kennis te nemen van de inhoud van het webforum. De Commissie beveelt aan dat de AIVD bij de verwerving van webfora in alle gevallen ten behoeve van de (interne) toestemming afweegt in hoeverre het kennis nemen van de inhoud van het desbetreffende webforum voldoet aan het noodzakelijkheids-, proportionaliteits- en subsidiariteitsvereiste. Deze afweging dient bovendien schriftelijk te worden vastgelegd.

Telefonieverkeersgegevens en gebruikersgegevens (paragraaf 3.6)

De AIVD en de MIVD zijn bevoegd telefonieverkeersgegevens op te vragen bij telecomproviders (artikel 28 Wiv 2002) en gebruikersgegevens bij het CIOT (artikel 29 Wiv 2002). Het opvragen van telefonieverkeersgegevens dient ingevolge artikel 28, vierde lid, Wiv 2002 door het hoofd van de dienst te geschieden. Ten aanzien van het opvragen van gebruikersgegevens op basis van artikel 29 Wiv 2002 staat de wet toe dat het hoofd van de dienst deze bevoegdheid mandateert. Er is geen wettelijke plicht om dit te motiveren. Bij de diensten wordt intern wel gemotiveerd om toestemming gevraagd. Daar de inzet van de bevoegdheden zich richt op een bepaald onderzoekssubject, is er geen sprake van het ongericht opvragen van (verzamelingen) telefonieverkeersgegevens en/of gebruikersgegevens. De verkregen telefonieverkeersgegevens worden geheel of gedeeltelijk tussen de AIVD en de MIVD gedeeld. Daarbij wordt voldaan aan de van toepassing zijnde wettelijke vereisten.

Het gebruik van gegevens op het gebied van telecommunicatie door de AIVD en de MIVD

De opslag en ontsluiting van gegevens op het gebied van telecommunicatie (paragraaf 4.1)

Er is een onderscheid tussen ruwe en geëvalueerde gegevens. Ruwe gegevens zijn nog niet geëvalueerd op relevantie in het kader van het doel waarvoor zij zijn verworven of een ander lopend onderzoek van de dienst. Ruwe gegevens die ongericht zijn geïntercepteerd mogen ingevolge de wet maximaal een jaar worden bewaard ten behoeve van nadere selectie (artikel 27 lid 9 Wiv 2002). Voor andere ruwe gegevens die door middel van de inzet van bijzondere bevoegdheden zijn verworven, zoals tapgegevens of gegevensverzamelingen die met een hack zijn verkregen, is geen bewaartermijn opgenomen in de Wiv 2002. De Commissie acht het in het kader van de bescherming van de persoonlijke levenssfeer van belang dat de wet nadere aanknopingspunten biedt voor de maximale bewaartermijn van ruwe gegevens in andere gevallen. Zij beveelt aan dat dit punt wordt betrokken bij de komende wijziging van de Wiv.

De algemene werkwijze van de AIVD en de MIVD voor de ontsluiting van ruwe gegevens die door de inzet van bijzondere bevoegdheden zijn verkregen sluit aan bij de wettelijke

vereisten voor interne toegang. Medewerkers van de diensten krijgen toegang tot gegevens voor zover dat noodzakelijk is voor een goede uitvoering van hun taak (artikel 35 Wiv 2002). De hoofden van de diensten dragen zorg voor de nodige beveiligingsvoorzieningen tegen onbevoegde gegevensverwerking (artikel 16 sub b Wiv 2002).

De analyse van gegevens op het gebied van telecommunicatie (paragraaf 4.2)

De Commissie is van oordeel dat de ruwe opbrengst van bijzondere bevoegdheden alleen mag worden gebruikt in het kader van het onderzoek waarbinnen de gegevens zijn verworven of ten behoeve van een ander lopend onderzoek dat onder de inlichtingen- of veiligheidstaken van de diensten valt (zie artikel 18 Wiv 2002). Dit om de inbreuk die op de persoonlijke levenssfeer wordt gemaakt door de inzet van bijzondere bevoegdheden te beperken. Wanneer gegevens eenmaal geëvalueerd zijn, mogen zij vervolgens in het kader van alle taken van de diensten (dus ook andere dan de inlichtingen- en veiligheidstaken) worden aangewend.

Bij de AIVD wordt gebruik gemaakt van applicaties die voor analysedoeleinden toegang verschaffen tot samengevoegde metagegevens vanuit verschillende bronnen, waaronder ruwe metagegevens die door de inzet van bijzondere bevoegdheden zijn verkregen. Voor zover deze analyse plaatsvindt in het kader van lopende onderzoeken die onder de inlichtingen- of veiligheidstaken van de AIVD vallen, is de Commissie van oordeel dat het gebruik van de samengevoegde metagegevens rechtmatig is. Dit betekent dat deze metagegevens niet mogen worden aangewend voor andere andere dan de inlichtingen- en veiligheidstaken van de dienst.

Het gebruik van gegevens uit webfora door de AIVD (paragraaf 4.3)

Webfora blijven doorgaans bewaard en beschikbaar binnen de AIVD. De Commissie acht dit een zwaar middel, zeker waar het gaat om fora waarvan niet iedere deelnemer op voorhand als (potentieel) onderzoekssubject aangemerkt kan worden. Het dient in verhouding te staan tot het operationele doel daarvan. De rechtmatigheid van het bewaren van webfora wordt in concrete gevallen beoordeeld in het onderzoek dat de Commissie thans uitvoert naar de onderzoeksactiviteiten van de AIVD op sociale media. Het toezichtsrapport betreffende dit onderzoek zal naar verwachting begin april 2014 worden voorgelegd aan de minister.

De uitwisseling van gegevens op het gebied van telecommunicatie met buitenlandse inlichtingen- en veiligheidsdiensten door de AIVD en de MIVD

Samenwerkingsrelaties met buitenlandse inlichtingen- en veiligheidsdiensten (paragraaf 5.1)

De uitwisseling van verzamelingen (ruwe) gegevens vindt plaats binnen hechte samenwerkingsrelaties waarbij wederzijds vertrouwen het uitgangspunt is. Het is in internationaal verband niet gebruikelijk te informeren naar de bron of de methode die gebruikt is om gegevens te vergaren of om hierover informatie te verstrekken.

De Commissie constateert dat de AIVD en de MIVD in de onderzochte hechte samenwerkingsverbanden er in grote mate op vertrouwen dat de desbetreffende buitenlandse diensten mensenrechten respecteren en handelen binnen de eigen nationale regelgeving. De Commissie is van mening dat het in het licht van de onthullingen van de afgelopen periode gewenst is na te gaan of dit vertrouwen nog steeds terecht is.

Voortvloeiend uit de wet[59] is het aan de hoofden van de AIVD en de MIVD onder de politieke verantwoordelijkheid van de betrokken minister te overwegen of buitenlandse diensten nog steeds in aanmerking komen voor de verschillende vormen van samenwerking die plaatsvinden in het kader van de hechte samenwerkingsrelatie.[60] Concreet betekent dit dat zij zich nader dienen te informeren over de wettelijke bevoegdheden en (technische) mogelijkheden van buitenlandse diensten, opdat zij verantwoorde afwegingen kunnen maken. De Commissie beveelt de ministers van BZK en van Defensie in dit verband aan de samenwerkingsrelaties (ook op internationaal niveau) te beoordelen op transparantie en de afwegingen die ten grondslag liggen aan de samenwerking nader te concretiseren

Internationale samenwerking vindt in het algemeen plaats op basis van het beginsel van *quid pro quo*, ofwel 'voor wat, hoort wat'. De AIVD en de MIVD zijn bevoegd gegevens te verstrekken of ondersteuning te verlenen. Hiervoor gelden de normen voor het verstrekken van (persoons)gegevens en de inzet van bijzondere bevoegdheden zoals de Wiv 2002 deze stelt. De AIVD en de MIVD mogen ook gegevens of ondersteuning ontvangen. De juridische toets die de Nederlandse diensten hierbij op basis van de Wiv 2002 moeten verrichten is beperkter.

<u>Het ontvangen van gegevens en ondersteuning door de AIVD en de MIVD</u> (paragraaf 5.2)

Sommige buitenlandse diensten hebben de bevoegdheid ook kabelgebonden telecommunicatie ongericht te intercepteren. De AIVD en de MIVD hebben die bevoegdheid niet. De vraag die hierbij rijst is of de AIVD en de MIVD, als zij met deze diensten samenwerken op het terrein van sigint, gebruik maken van een zogenaamde U-bochtconstructie. Immers zij kunnen zo toegang verkrijgen tot gegevens die worden verzameld met de inzet van een bevoegdheid waar zij zelf niet over beschikken. De Commissie is van oordeel dat dergelijke interceptie niet op zichzelf reeds een ongeoorloofde inbreuk op de persoonlijke levenssfeer oplevert. Aan de AIVD en de MIVD is immers in de Wiv 2002 een vergelijkbare bevoegdheid toegekend ten aanzien van niet-kabelgebonden telecommunicatie. Bij de totstandkoming van de Wiv 2002 is geen expliciete grondrechtelijke afweging gemaakt over het verschil tussen kabelgebonden en niet-kabelgebonden telecommunicatie. De Commissie acht het in dit verband toegestaan dat de AIVD en de MIVD samenwerken met deze buitenlandse diensten, ook als niet uitgesloten kan worden dat zij gegevens ontvangen die zijn verkregen door ongerichte interceptie van kabelgebonden telecommunicatie.

De Commissie heeft in haar onderzoek geen aanwijzingen gevonden dat de AIVD en de MIVD expliciet verzoeken hebben gericht aan buitenlandse diensten om methoden in te zetten die naar Nederlands recht niet geoorloofd zijn.

<u>Activiteiten van buitenlandse diensten op Nederlands grondgebied</u> (paragraaf 5.3)

De Wiv 2002 staat het buitenlandse diensten alleen toe activiteiten te ontplooien op Nederlands grondgebied indien hiervoor door de verantwoordelijke minister toestemming is gegeven en indien dit geschiedt onder supervisie en verantwoordelijkheid van de AIVD of

[59] In artikel 59 Wiv 2002 is de zorgplicht van de hoofden van de AIVD en de MIVD neergelegd voor het onderhouden van verbindingen met daarvoor in aanmerking komende buitenlandse diensten.
[60] Toezichtsrapport van de CTIVD nr. 22a inzake de samenwerking van de AIVD met buitenlandse inlichtingen- en/of veiligheidsdiensten, *Kamerstukken II* 2009/10, 29 924, nr. 39 (bijlage), beschikbaar op www.ctivd.nl, paragraaf 5.1 en 6.1.

de MIVD. De Commissie heeft geen aanwijzingen gevonden dat buitenlandse diensten met medewerking van de AIVD of de MIVD zelfstandige toegang hebben verkregen tot Nederlandse telefoon- of internetverbindingen.

Het uitwisselen van metagegevens door de AIVD en de MIVD ten aanzien van bepaalde onderwerpen (paragraaf 5.4)

Door de AIVD en de MIVD worden structureel (ruwe) metagegevens gedeeld binnen een internationaal samenwerkingsverband. De metagegevens zijn verworven door middel van ongerichte interceptie van niet-kabelgebonden telecommunicatie en kunnen persoonsgegevens betreffen. Daardoor is in potentie sprake van een inbreuk op de persoonlijke levenssfeer. De Commissie is van oordeel dat de verstrekking van de metagegevens binnen dit samenwerkingsverband voldoet aan het wettelijke vereiste van noodzakelijkheid in het kader van de taakuitvoering van de diensten. Bovendien weegt het doel van de verstrekking op tegen de inbreuk die kan worden gemaakt op de persoonlijke levenssfeer. Daarnaast heeft de Commissie geen aanwijzingen dat de diensten niet zorgvuldig tewerk gaan. De werkwijze van de AIVD en de MIVD bij de onderhavige structurele uitwisseling van gegevens is daarom rechtmatig naar het oordeel van de Commissie.

De inzet van de selectiebevoegdheid door de MIVD ten behoeve van partnerdiensten (paragraaf 5.5)

De MIVD verleent ondersteuning aan buitenlandse diensten door de inzet van de selectiebevoegdheid ten aanzien van ongericht geïntercepteerde niet-kabelgebonden communicatie. De MIVD merkt de ondersteuning echter niet aan als selectie. Om deze reden wordt ook niet per kenmerk een gemotiveerd verzoek aan de minister gericht. De bescherming van de persoonlijke levenssfeer vereist dat bij de inzet van bijzondere bevoegdheden invulling wordt gegeven aan de waarborgen die zijn neergelegd in de Wiv 2002, ook als die inzet plaatsvindt ter ondersteuning aan een buitenlandse dienst. De huidige werkwijze van de MIVD is naar het oordeel van de Commissie onrechtmatig. Zij beveelt dan ook aan dat de MIVD zijn werkwijze onverwijld aanpast zodat de minister voortaan op basis van een motivering aan de hand van de beschikbare informatie om toestemming wordt gevraagd voor de toepassing van de selectiebevoegdheid.

Het uitwisselen van webfora door de AIVD (paragraaf 5.6)

De AIVD wisselt met een aantal buitenlandse diensten webfora uit. Het gaat hierbij om verzamelingen persoonsgegevens waardoor sprake is van een inbreuk op de persoonlijke levenssfeer. Het betreft in vrijwel alle gevallen webfora die enkel de gegevens bevatten van (potentiële) onderzoekssubjecten van de dienst. De Commissie stelt ten aanzien van het verstrekken van dergelijke webfora in het algemeen dat dit noodzakelijk kan zijn in het kader van de taakuitvoering van de AIVD en aangemerkt kan worden als evenredig in verhouding tot het daarmee te dienen doel. Daarnaast heeft de Commissie geen aanwijzingen dat de AIVD niet zorgvuldig tewerk gaat. De werkwijze van de AIVD bij de onderhavige uitwisseling van gegevens is daarom rechtmatig naar het oordeel van de Commissie.

De rechtmatigheid van het verstrekken van webfora in concrete gevallen wordt beoordeeld in het onderzoek dat de Commissie thans uitvoert naar de onderzoeksactiviteiten van de

AIVD op sociale media. Het toezichtsrapport betreffende dit onderzoek zal naar verwachting begin april 2014 worden voorgelegd aan de minister.

Aldus vastgesteld in de vergadering van de Commissie d.d. 5 februari 2014.

CTIVD nr. 38

BIJLAGE

Juridisch kader gegevensverwerking

Bij het openbare toezichtsrapport inzake gegevensverwerking op het gebied van telecommunicatie door de AIVD en de MIVD

I Inleiding

De werkzaamheden van de AIVD en de MIVD richten zich in de kern op het verwerken van gegevens, zowel persoonsgegevens[61] als andere gegevens.[62] Gegevensverwerking is een ruim begrip. In de wet die het handelen van de diensten reguleert, de Wet op de inlichtingen- en veiligheidsdiensten 2002 (Wiv 2002), wordt hieronder verstaan het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens.[63] In het kader van het doen van onderzoek door de diensten komt dit in essentie neer op het verzamelen van gegevens en op het analyseren en eventueel exploiteren van die gegevens. Bij het verrichten van de gegevensverwerkende activiteiten, met name het verzamelen van gegevens door de inzet van bijzondere bevoegdheden, kan direct inbreuk worden gemaakt op de fundamentele rechten van burgers die daarvan in de regel onwetend zijn vanwege het heimelijke karakter van de activiteiten. Bij de verwerking van persoonsgegevens wordt steeds in meer of mindere mate een inbreuk op de persoonlijke levenssfeer van de onderzochte personen gemaakt. Met de Wiv 2002 heeft de wetgever beoogd een balans te vinden tussen enerzijds het belang van de nationale veiligheid en de taken en bevoegdheden van de diensten in dat verband en anderzijds het belang van bescherming van grondrechten (die burgers vrijwaren van te vergaand overheidsingrijpen) en democratische controle op het functioneren van de diensten.

In dit verband wordt gewezen op de evaluatie van de Wiv 2002 door een speciale evaluatiecommissie: de Commissie-Dessens. Het rapport van deze commissie is begin december 2013 gepresenteerd aan de betrokken ministers.[64] Hierin wordt onder meer voorgesteld om de bevoegdheden van de diensten op het terrein van kabelgebonden communicatie uit te breiden in aansluiting op technologische ontwikkelingen en tevens het toezicht van de Commissie van Toezicht betreffende de Inlichtingen- en Veiligheidsdiensten (CTIVD) op de rechtmatigheid van het optreden van de diensten te versterken. Op dit punt wordt volstaan met deze vermelding.

---

[61] In artikel 1, onder e, Wiv 2002 zijn persoonsgegevens gedefinieerd als gegevens die betrekking hebben op een identificeerbare of geïdentificeerde, individuele natuurlijke persoon.

[62] Waar in dit hoofdstuk wordt gesproken van "gegevens", ziet het begrip op persoonsgegevens en andere gegevens. Het begrip ziet zowel op individuele gegevens als gegevensverzamelingen.

[63] Artikel 1, onder f, Wiv 2002.

[64] Rapport Commissie-Dessens, *Evaluatie Wet op de inlichtingen- en veiligheidsdiensten 2002. Naar een nieuwe balans tussen bevoegdheden en waarborgen*, december 2013, *Kamerstukken II* 2013/14, 33 820, nr. 1 (bijlage).

Deze bijlage is als volgt opgebouwd. Eerst wordt ingegaan op de totstandkoming van de Wiv 2002 en de mensenrechtelijke overwegingen die hieraan ten grondslag liggen. Hierbij wordt ook toegelicht hoe de bescherming van mensenrechten, met name het recht op eerbiediging van de persoonlijke levenssfeer en het telefoon- en telegraafgeheim, in het Europees Verdrag voor de Rechten van de Mens (EVRM) en de daarbij behorende jurisprudentie en in de Grondwet is geregeld (paragraaf II). Daarna worden de waarborgen die in de Wiv 2002 zijn opgenomen ter bescherming van deze fundamentele rechten van burgers toegelicht (paragraaf III). In lijn met de structuur van de Wiv 2002, wordt vervolgens ingegaan op de algemene bevoegdheid van de diensten tot gegevensverwerking en de vereisten die de wet hieraan stelt (paragraaf IV). In aansluiting hierop worden twee specifieke vormen van gegevensverwerking besproken. Eerst, de algemene en bijzondere bevoegdheden die de wet de diensten biedt om gegevens te verzamelen in het belang van de nationale veiligheid en de begrenzingen en voorwaarden die daarbij gelden. De bijzondere bevoegdheden op het gebied van telecommunicatie worden hierbij afzonderlijk toegelicht (paragraaf V). Daarna, wordt ingegaan op de samenwerking van de AIVD en de MIVD met buitenlandse inlichtingen- en/of veiligheidsdiensten (paragraaf VI).

II Persoonlijke levenssfeer versus inlichtingen & veiligheid

II.1 Totstandkoming van de Wiv 2002

De huidige Wiv 2002 vindt zijn oorsprong in twee uitspraken van de Afdeling bestuursrechtspraak van de Raad van State (ABRS) in 1994 waarin de toenmalige Wet op de inlichtingen- en veiligheidsdiensten 1987 in strijd werd geoordeeld met de artikelen 8 en 13 van het EVRM.[65] In artikel 8 EVRM is het recht op eerbiediging van de persoonlijke levenssfeer neergelegd. Artikel 13 EVRM bepaalt dat een ieder die een aannemelijke claim heeft dat zijn mensenrechten zijn geschonden recht heeft op een daadwerkelijk rechtsmiddel voor een nationale instantie. Het Europees Hof voor de Rechten van de Mens (EHRM) heeft in zijn jurisprudentie een invulling gegeven van de voorwaarden die uit de genoemde rechten voortvloeien. Een aantal uitspraken heeft betrekking op geheim onderzoek door inlichtingen- en veiligheidsdiensten. Samenvattend houdt deze jurisprudentie in dat:
1) een systeem dat geheim onderzoek naar personen toelaat bij de wet geregelde en voldoende waarborgen dient te bieden, zoals duidelijkheid en voorzienbaarheid in de zin dat een burger kan begrijpen onder welke omstandigheden de overheid een bepaalde inbreukmakende bevoegdheid mag uitoefenen en onder welke voorwaarden dat mag gebeuren (artikel 8)[66], en
2) de heimelijkheid van het werk van inlichtingen- en veiligheidsdiensten weliswaar beperkingen meebrengt voor het toezicht daarop, maar dat op nationaal niveau een (niet noodzakelijkerwijze juridisch) systeem dient te bestaan dat in zijn geheel voldoende waarborgt dat een effectief rechtsmiddel openstaat tegen mogelijke mensenrechtenschendingen als gevolg van geheim onderzoek door inlichtingen- en veiligheidsdiensten (artikel 13).[67]

---

[65] ABRvS 9 juni 1994, *Van Baggum & Valkenier*, AB 1995/238.
[66] EHRM 26 april 1979, *Sunday Times t. Verenigd Koninkrijk*, § 49; EHRM 25 maart 1983, *Silver e.a. t. Verenigd Koninkrijk*, § 85; EHRM 2 augustus 1984, *Malone t. Verenigd Koninkrijk*, § 68; EHRM 24 april 1990, *Kruslin t. Frankrijk*, § 33 en 35; EHRM 24 april 1990, *Huvig t. Frankrijk*, § 32 en 34.
[67] EHRM 6 september 1978, *Klass e.a. t. Duitsland*, § 67; *Silver e.a. t. Verenigd Koninkrijk*, § 113.

In navolging van deze jurisprudentie oordeelde de ABRS dat weliswaar in de toenmalige Wiv (1987) was geregeld ten aanzien van welke (categorieën van) personen het verwerken van gegevens (geheim onderzoek) was toegestaan maar dat onvoldoende was geregeld onder welke omstandigheden dat mocht plaatsvinden en welke middelen hiervoor ter beschikking stonden. Daarom was volgens de ABRS niet voldaan aan het vereiste uit artikel 8, tweede lid, EVRM dat een inmenging in de persoonlijke levenssfeer van burgers slechts mag plaatsvinden indien deze bij de wet is voorzien. Daarnaast oordeelde de ABRS dat in Nederland een daadwerkelijk rechtsmiddel in de zin van artikel 13 EVRM ontbrak ten aanzien van schendingen van grondrechten door geheim onderzoek door de toenmalige inlichtingen- en veiligheidsdiensten. De toen bestaande toezichtmechanismen, in het bijzonder de klachtregeling bij de Nationale ombudsman en het parlementaire toezicht door de vaste commissie voor de Inlichtingen- en Veiligheidsdiensten van de Tweede Kamer (commissie IVD), werden onvoldoende geoordeeld als daadwerkelijk rechtsmiddel omdat de Nationale ombudsman niet bevoegd is tot het geven van bindende beslissingen en parlementair toezicht slechts voldoet aan de uit het EVRM voortvloeiende eisen indien deze waarborg in de wet is geregeld, die wettelijke regeling aan de eisen uit artikel 8, tweede lid, EVRM voldoet en er een regeling is om de onderzochte persoon op enig tijdstip van het feit dat hij onderwerp van een onderzoek is geweest op de hoogte te brengen. De uitspraken van de ABRS leidden tot een kabinetsstandpunt.[68] In 1998 werd een wetsvoorstel voor een nieuwe wet ingediend bij de Tweede Kamer.[69] In de nieuwe wet, die in mei 2002 in werking trad, werd tegemoet gekomen aan de kritiek van de ABRS door afbakening en beschrijving van de omstandigheden waarin ten aanzien van specifieke categorieën van personen onderzoek mag worden verricht teneinde gegevens te verwerken, door opname en beschrijving van de bijzondere bevoegdheden die daarbij – onder specifieke voorwaarden – mogen worden ingezet en door het instellen van een gespecialiseerde en onafhankelijke toezichthouder. Hierbij speelt mee dat het grootste deel van het wetgevingstraject plaatsvond in een tijd waarin de nadruk meer lag op het uitbreiden van waarborgen en toezicht dan op uitbreiding van bevoegdheden van de diensten.[70] Op deze wijze heeft de wetgever beoogd het belang van inlichtingen en veiligheid enerzijds en het belang van eerbiediging van grondrechten (met name de persoonlijke levenssfeer) anderzijds op een goede wijze te verenigen en te balanceren in de Wiv 2002.

II.2 Jurisprudentie van het EHRM over artikel 8 en inlichtingen- & veiligheidsdiensten[71]

Over de jurisprudentie van het EHRM ten aanzien van artikel 8 EVRM valt veel te zeggen, met name vanwege de grote hoeveelheid uitspraken en de brede interpretatie die het EHRM geeft aan de in deze bepaling opgenomen rechten. Vanwege de nauwe relatie van het onderwerp van het onderzoek in dit rapport met de rechten uit artikel 8 EVRM, in het bijzonder het recht op bescherming van de persoonlijke levenssfeer, is ervoor gekozen op hoofdlijnen in te gaan op de jurisprudentie van het EHRM daarover. Er is met name gekeken naar de uitspraken waarin het EHRM zich heeft uitgesproken over de vragen in welke gevallen sprake is van inmenging in het recht op bescherming van de persoonlijke levenssfeer door geheim onderzoek van een inlichtingen- en/of veiligheidsdienst en onder

[68] *Kamerstukken II* 1994/95, 22 036, nr. 6.
[69] *Kamerstukken II* 1994/05, 25 877, nr. 2.
[70] H.T. Bos-Ollermann, 'Meerdere wegen naar Straatsburg. Geheime methoden en toezicht op de inlichtingen- en veiligheidsdiensten in België en Nederland', in *De orde van de dag*, afl. 56 (dec. 2011), p. 100.
[71] De uitspraken van het EHRM zijn beschikbaar op www.echr.coe.int via de zoekmachine HUDOC.

welke voorwaarden deze inmenging gerechtvaardigd kan zijn op grond van het belang van de nationale veiligheid.

II.2.1 Inmenging

In artikel 8, eerste lid, EVRM is vastgelegd dat een ieder recht heeft op respect voor zijn privéleven, zijn familie- en gezinsleven, zijn woning en zijn correspondentie. De elementen zijn afzonderlijk genoemd maar hebben een duidelijke onderlinge interactie omdat ze in elkaars verlengde liggen en ook een zekere overlap bevatten. Een telefoontap kan zowel een inmenging in het privéleven van een persoon, als in zijn correspondentie, en misschien zelfs in zijn woning, inhouden.[72] Voor de toepasselijkheid van artikel 8 EVRM is het van belang dat een vermeende schending binnen de reikwijdte van (een of meerdere van) de rechten uit die bepaling valt, met andere woorden dat sprake is van een inmenging in de genoemde rechten. In de bepaling zijn geen definities opgenomen. De jurisprudentie biedt echter nader inzicht in de interpretatie die aan de rechten in artikel 8 is gegeven.

Uit de uitspraken die specifiek betrekking hebben op geheim onderzoek van een inlichtingen- en/of veiligheidsdienst in het kader van de nationale veiligheid valt af te leiden dat het EHRM in deze zaken al snel tot de conclusie komt dat er een inmenging heeft plaatsgevonden in de rechten van de onderzochten genoemd in artikel 8 EVRM. Het EHRM neemt tot uitgangspunt dat het enkele bestaan van wetgeving dat een systeem van heimelijke surveillance en interceptie van telecommunicatie toestaat, een inmenging vormt in de uitoefening van de rechten onder artikel 8 EVRM van personen op wie de wetgeving betrekking kan hebben, los van de vraag of daadwerkelijk middelen zijn ingezet.[73] Hierbij dient in ogenschouw te worden genomen of er een mogelijkheid is de toepassing van die bevoegdheden op nationaal niveau aan te vechten.[74] Het EHRM heeft verschillende vormen van (tele)communicatie onder de reikwijdte van het recht op bescherming van de persoonlijke levenssfeer en correspondentie gebracht, niet alleen inhoudelijke communicatie zoals telefoongesprekken, poststukken, facsimile en e-mailcommunicatie[75], maar ook verkeersgegevens, dat wil zeggen gegevens die niet de inhoud van de communicatie betreffen.[76] Ook heeft het EHRM het opslaan van gegevens over het privéleven van burgers

---

[72] C. Ovey & R. White, *Jacobs & White The European Convention on Human Rights (4th Edition)*, Oxford: Oxford University Press 2006, p. 242.

[73] *Klass e.a. t. Duitsland*, § 41; *Malone t. Verenigd Koninkrijk*, § 64; EHRM (dec.) 29 juni 2006, *Weber en Saravia t. Duitsland*, § 77-78; EHRM 1 juli 2008, *Liberty e.a. t. Verenigd Koninkrijk* § 56; EHRM 25 mei 2011, *Association "21 Decembre 1989" e.a. t. Roemenië*, § 114.

[74] EHRM 18 mei 2010, *Kennedy t. Verenigd Koninkrijk*, § 124.

[75] *Klass e.a. t. Duitsland*, § 41; *Malone t. Verenigd Koninkrijk*, § 64; *Weber en Saravia t. Duitsland*, § 77-78; *Liberty e.a. t. Verenigd Koninkrijk,* § 56; *Association "21 Decembre 1989" e.a. t. Roemenië*, § 114.

[76] In *Malone t. Verenigd Koninkrijk* ging de klacht over het tappen van klagers telefoongesprekken en het monitoren van de nummers die hij koos. Ten aanzien van het laatstgenoemde punt overwoog het EHRM: "(…) a meter check printer registers information that a supplier of a telephone service may in principle legitimately obtain, notably in order to ensure that the subscriber is correctly charged or to investigate complaints or possible abuses of the service. By its very nature, metering is therefore to be distinguished from interception of communications, which is undesirable and illegitimate in a democratic society unless justified. The Court does not accept, however, that the use of data obtained from metering, whatever the circumstances and purposes, cannot give rise to an issue under Art. 8. The records of metering contain information, in particular the numbers dialled, which is an integral element in the communications made by telephone. Consequently, release of that information to the police without the consent of the subscriber also amounts, in the opinion of the Court, to an interference with a right guaranteed by Art. 8." (§ 84). In EHRM 3 april 2007, *Copland t. Verenigd Koninkrijk* werd geklaagd over het monitoren van klaagsters telefoongesprekken, e-mailverkeer en

in geheime overheidsdatabases onder de reikwijdte van artikel 8 gebracht.[77] Volgens het EHRM kan publieke informatie onderdeel van het privéleven worden indien de data systematisch verzameld en opgeslagen worden in overheidsdossiers.[78] Voor wat betreft de vormen van interceptie heeft het EHRM zich niet alleen uitgesproken over het gericht verzamelen van gegevens ten aanzien van personen, maar ook over het verzamelen en opnemen van ongericht geïntercepteerde telecommunicatiegegevens (zogenaamde *strategic monitoring*)[79] en over het ongericht intercepteren van telefoongesprekken, facsimile en e-mail en selectie daarvan naderhand op basis van trefwoorden of selectiecriteria.[80] Het bestaan van bepaalde bevoegdheden, in het bijzonder de bevoegdheden tot het doen van onderzoek naar, het gebruik en de opslag van de geïntercepteerde communicatie, kan volgens het EHRM een inmenging vormen in de uitoefening van de rechten onder artikel 8 EVRM.[81] Ook de verdere verstrekking van de geïntercepteerde persoonsgegevens kan tot een op zichzelf staande inmenging in de uitoefening van de rechten in artikel 8 EVRM leiden.[82]

II.2.2 Rechtvaardiging van de inmenging

Artikel 8 EVRM verbiedt weliswaar iedere inmenging van de overheid in de uitoefening van de rechten in deze bepaling, maar op grond van het tweede lid kan een inmenging gerechtvaardigd zijn voor zover deze bij de wet is voorzien en in een democratische samenleving noodzakelijk is in het belang van onder meer de nationale veiligheid. Deze voorwaarden zijn nader uitgewerkt in de omvangrijke jurisprudentie van het EHRM over artikel 8 EVRM. Op hoofdlijnen komt het op het volgende neer.

Ten eerste dient de inmenging een basis te hebben in nationale wetgeving, waarbij het niet alleen om formele wetgeving maar juist ook om materiële regelgeving kan gaan.[83] Ook dient deze wetgeving toegankelijk en voorzienbaar te zijn.[84] Dit houdt in dat de regels waarop het inbreukmakende optreden is gebaseerd op afdoende wijze zijn gepubliceerd of bekend zijn gemaakt[85] en dat de regels voldoende duidelijk en nauwkeurig zijn. Vanuit het oogpunt dat heimelijk onderzoek het risico inhoudt dat misbruik van bevoegdheden wordt gemaakt, geldt het voorgaande volgens het EHRM des te meer daar waar de toe te passen technologie

---

internetgebruik door haar werkgever op haar werkplek. Hierbij overwoog het EHRM – onder verwijzing naar *Malone* – dat "the use of information relating to the date and length of telephone conversations and in particular the number dialled can give rise to an issue under article 8 as such information constitutes an "integral element of the communications made by telephone"(…). The collection and storage of personal information relating to the applicant's telephone, as well as to her e-mail and internet usage, without her knowledge, amounted to an interference with her right to respect for her private life and correspondence." (§ 43).

[77] *Association "21 Decembre 1989" e.a. t. Roemenië*, § 115.

[78] EHRM 4 mei 2000, *Rotaru t. Roemenië*, § 43.

[79] *Weber en Saravia t. Duitsland*, § 4.

[80] *Liberty e.a. t. Verenigd Koninkrijk*, § 1.

[81] *Idem*, § 57.

[82] *Weber en Saravia t. Duitsland*, § 79: "(…) the transmission of data to and their use by other authorities, which enlarges the group of persons with knowledge of the personal data intercepted and can lead to investigations being instituted against the persons concerned, constitutes a further separate interference with the applicants' rights under Article 8 (…)."

[83] *Sunday Times t. Verenigd Koninkrijk*, § 47; *Kruslin t. Frankrijk*, § 29; *Huvig t. Frankrijk*, § 28.

[84] *Sunday Times t. Verenigd Koninkrijk*, § 49; *Silver e.a. t. Verenigd Koninkrijk*, § 85; *Kruslin t. Frankrijk*, § 27; *Huvig t. Frankrijk*, § 26.

[85] *Silver e.a. t. Verenigd Koninkrijk*, § 87; EHRM 26 maart 1987, *Leander t. Zweden*, § 53.

steeds geavanceerder wordt.[86] De mate van de vereiste duidelijkheid en nauwkeurigheid van de regelgeving is volgens het EHRM afhankelijk van het specifieke onderwerp. Regelgeving in het kader van de nationale veiligheid, bijvoorbeeld over de bevoegdheid communicatie af te tappen of geheim onderzoek te doen, kan daarom aan de burger niet dezelfde duidelijkheid en nauwkeurigheid bieden als regelgeving op andere terreinen.[87] Bovendien komt de overheid hierbij vaak een bepaalde beoordelingsvrijheid toe. Dit is soms onvermijdelijk. Het EHRM stelt dat, vanuit het oogpunt van de *rule of law*, de regelgeving dan wel een indicatie moet bevatten van de omvang van die beoordelingsruimte.[88] Daarnaast moeten er voldoende waarborgen in het rechtssysteem aanwezig zijn om de burger te beschermen tegen willekeur.[89] Dit vereist allereerst dat de wet in ieder geval dusdanig duidelijk is dat de burger kan begrijpen onder welke omstandigheden de overheid een bepaalde inbreukmakende bevoegdheid mag uitoefenen en onder welke voorwaarden dat mag gebeuren.[90] Daarnaast hecht het EHRM belang aan de aanwezigheid van adequate juridische procedures om vermeende willekeurige inmenging aan te kunnen vechten.[91] Het EHRM heeft deze uitgangspunten vertaald naar een aantal minimumwaarborgen ten aanzien van het gericht tappen van telecommunicatie (dat wil zeggen bevoegdheden gericht op specifieke personen) die vervolgens tevens van toepassing zijn geoordeeld op bevoegdheden die meer ongericht zijn, zoals ongerichte interceptie van telecommunicatie.[92] De nationale regelgeving moet in ieder geval regels omvatten over de aard van de activiteiten die de aanleiding kunnen vormen voor interceptie, de categorieën personen wier communicatie geïntercepteerd kan worden, een beperking van de duur van de interceptie, de te volgen procedure voor het onderzoek, gebruik en de opslag van geïntercepteerde gegevens, de te nemen voorzorgsmaatregelen bij externe verstrekking van de gegevens en de omstandigheden waaronder de gegevens verwijderd of vernietigd mogen of moeten worden.[93]

Ten tweede behoort de inmenging een legitiem doel te dienen. De doelen staan uitputtend genoemd in het tweede lid van artikel 8 EVRM. In dit onderzoek is met name de nationale veiligheid als legitiem doel van belang. Het is in beginsel aan de staat zelf om de initiële beoordeling te maken of er een gerechtvaardigd belang door de inmenging gediend wordt.[94] Aan de nationale autoriteiten komt op dit punt een ruime beoordelingsvrijheid (*wide margin*

---

[86] *Weber en Saravia t. Duitsland*, § 93; EHRM 2 september 2010, *Uzun t. Duitsland*, § 61; EHRM 21 juni 2011, *Shimovolos t. Rusland*, § 68.
[87] *Malone t. Verenigd Koninkrijk*, § 67; *Leander t. Zweden*, § 51.
[88] *Silver e.a. t. Verenigd Koninkrijk*, § 88.
[89] *Malone t. Verenigd Koninkrijk*, § 67.
[90] *Malone t. Verenigd Koninkrijk*, § 68; *Kruslin t. Frankrijk*, § 33 en 35; *Huvig t. Frankrijk*, § 32 en 34.
[91] *Rotaru t. Roemenië*, § 59.
[92] In de Europese Unie heeft een door het Europees Parlement ingestelde onderzoekscommissie zich in 2000 gebogen over de vraag welke potentiële impact het ECHELON interceptie systeem op de rechten van individuen onder de wet- en regelgeving van de EU had. Het ECHELON programma werd gezamenlijk uitgevoerd door de Verenigde Staten, het Verenigd Koninkrijk, Australië, Canada en Nieuw-Zeeland en richtte zich op ongerichte interceptie van communicatieverkeer via satellieten. De conclusie van de onderzoekscommissie luidde dat: "(…) mass interception systems such as ECHELON have the potential to violate the right to privacy because they do not comply with the principle of proportionality with regard to the use of intrusive methods. While acknowledging that such interception systems may be justified on national security grounds, the committee recommends that their use be governed by clear and accessible legislation and that EU member states establish rigorous oversight."
[93] *Weber en Saravia t. Duitsland*, § 95; *Liberty e.a. t. Verenigd Koninkrijk*, § 62 en 63.
[94] EHRM 7 december 1976, *Handyside t. Verenigd Koninkrijk*, § 48 en 49; *Sunday Times t. Verenigd Koninkrijk*, § 59.

of appreciation) toe. Het begrip "nationale veiligheid" komt ook terug in de Wiv 2002 als het kader waarbinnen de taken van de diensten dienen plaats te vinden. Het EHRM definieert de inhoud en de reikwijdte van het begrip niet,[95] maar beoordeelt per geval of een verdragsstaat terecht een beroep heeft gedaan op de nationale veiligheid als grond om een inbreuk op een mensenrecht te rechtvaardigen. In verscheidene uitspraken zijn vormen van bedreigingen van de nationale veiligheid vastgesteld. Zo kan de nationale veiligheid onder meer in gevaar worden gebracht door spionage[96], separatistische bewegingen[97], terrorisme[98], het aanzetten tot en het goedkeuren van terrorisme[99], het publiceren van staatsgeheimen[100] en aantasting van de integriteit van het ambtelijk apparaat[101]. Jurisprudentie van het EHRM toont dat er voor de rechtvaardiging van geheim onderzoek door inlichtingen- en veiligheidsdiensten in het belang van de nationale veiligheid geen sprake hoeft te zijn van een daadwerkelijke aantasting van de nationale veiligheid. Wel dient er minstens sprake te zijn van de mogelijkheid dat de nationale veiligheid wordt aangetast, met andere woorden een potentiële aantasting van de nationale veiligheid. Als er in het geheel geen aantasting van de nationale veiligheid verwacht kan worden, dan kan een inbreuk op de persoonlijke levenssfeer niet worden gerechtvaardigd.[102]

Ten derde dient de inmenging noodzakelijk te zijn in een democratische samenleving. Om te kunnen voldoen aan het noodzakelijkheidscriterium dient er volgens de jurisprudentie van het EHRM sprake te zijn van een dringende maatschappelijke behoefte (*pressing social need*) die de inbreuk op het mensenrecht rechtvaardigt.[103] Of daarvan sprake is dient van geval tot geval te worden beoordeeld. Het begrip noodzaak dient restrictief te worden geïnterpreteerd, wat in het geval van geheim onderzoek betekent dat de inbreuk strikt noodzakelijk moet zijn in een democratische samenleving.[104] Het middel waarmee inbreuk wordt gemaakt op de rechten van een persoon dient bij te dragen aan het doel waarvoor het wordt ingezet om de inzet van het middel als noodzakelijk te kunnen aanmerken. Hiertoe dient sprake te zijn van proportionaliteit (dat wil zeggen een redelijke verhouding) tussen de inmenging en de bescherming van het doel dat met de inmenging wordt beoogd te bereiken.[105] De inmenging mag niet van zodanige aard zijn dat de essentie van het recht wordt uitgehold. En wanneer met een lichtere inbreukmakende maatregel kan worden volstaan (ook wel het subsidiariteitsvereiste genoemd), is de inmenging niet proportioneel.[106] In overeenstemming met het subsidiaire karakter van het Straatsburgse mechanisme, wordt aan de staat een zekere beoordelingsruimte gelaten bij het inzetten van middelen in het belang van de nationale veiligheid, mits er voldoende waarborgen tegen willekeur zijn.[107] De afweging of er voldoende waarborgen zijn is afhankelijk van alle omstandigheden van het

---

[95] In navolging van de uitspraak van de Europese Commissie voor de Rechten van de Mens (ECRM) 2 april 1993, *Esbester t. Verenigd Koninkrijk*.
[96] *Klass t. Duitsland*, § 48.
[97] EHRM 30 januari 1998, *United Communist Party of Turkey e.a. t. Turkije*, § 33-36.
[98] *Klass t. Duitsland*, § 48.
[99] EHRM 19 december 1997, *Zana t. Turkije*, § 48-50.
[100] EHRM 26 november 1991, *Observer en The Guardian t. Verenigd Koninkrijk*.
[101] EHRM 12 december 2001, *Grande Oriente d'Italia di Palazzo Giustiniani t. Italië*, § 21.
[102] Zie o.a. *Klass e.a. t. Duitsland*; *Leander t. Zweden*.
[103] Zie o.a. *Leander t. Zweden*, § 58.
[104] *Klass e.a. t. Duitsland*, § 48; *Rotaru t. Roemenië*, § 47; EHRM 6 juni 2006, *Segerstedt-Wiberg e.a. t. Zweden*, § 88 en *mutatis mutandis* voor geheim onderzoek in het kader van het strafrecht: EHRM 2 november 2006, *Volkhy t. Oekraïne*, § 43.
[105] *Handyside t. Verenigd Koninkrijk*, § 49.
[106] EHRM 2 oktober 2001, *Hatton e.a. t. Verenigd Koninkrijk*, § 97.
[107] *Klass e.a. t. Duitsland*, § 46 en 48-50; *Leander t. Zweden*, § 59 en 60; *Malone t. Verenigd Koninkrijk*, § 81.

geval, waaronder de aard, het bereik en de duur van de bevoegdheid, de gronden op basis waarvan de bevoegdheid mag worden ingezet, de autoriteiten die bevoegd zijn toestemming te verlenen, de bevoegdheid uit te oefenen en toezicht te houden, alsmede het rechtsmiddel dat in het nationale rechtssysteem aan het individu openstaat.[108] Hierbij vindt het EHRM van belang dat de nationale regelgeving waarborgen bevat die garanderen dat heimelijk verkregen data worden vernietigd op het moment dat ze niet langer nodig zijn om het beoogde doel te bereiken (hiervoor acht het EHRM van belang dat de inbreukmakende maatregel intern is voorzien van een voldoende specifieke doelstelling).[109]

II.3 Bescherming van de persoonlijke levenssfeer in de Grondwet

De bescherming van de persoonlijke levenssfeer is in de Grondwet allereerst geregeld in artikel 10 waarin in het eerste lid in algemene zin is opgenomen dat een ieder recht heeft op eerbiediging van zijn persoonlijke levenssfeer. In het eerste lid is eveneens opgenomen dat bij of krachtens de wet beperkingen kunnen worden gesteld. De precieze reikwijdte van de bescherming van de persoonlijke levenssfeer wordt dus in andere wetten, zoals in de Wiv 2002, nader geregeld.

Artikel 13 van de Grondwet vormt een specifieke uitwerking van een deel van de bescherming van de persoonlijke levenssfeer. Artikel 13 verklaart dat het briefgeheim (lid 1) en het telefoon- en telegraafgeheim (lid 2) onschendbaar zijn. Voor het onderhavige onderzoek zijn vooral het telefoon- en telegraafgeheim van belang. Beperkingen van het telefoon- en telegraafgeheim vereisen een voorafgaande machtiging door een bevoegd orgaan. Zo is in de Wiv 2002 opgenomen dat sommige bijzondere bevoegdheden pas mogen worden ingezet indien door de betrokken minister daarvoor toestemming is verleend.

Het telefoon- en telegraafgeheim in artikel 13 Grondwet beschermen de verzender van een boodschap die via telefonie of telegrafie verloopt tegen de kennisneming van de inhoud van de communicatie door degene die met de verzending is belast of tegen degene die via de transporteur toegang tot de verzonden boodschap heeft. Omdat soms om technische redenen kennis wordt genomen van de communicatie, heeft het geheim ook de strekking dat de inhoud van de communicatie niet verder wordt verspreid. Het telefoon- en telegraafgeheim beschermen besloten (privé)communicatie. Dat wil zeggen dat de verzender het nodige moet hebben gedaan om de communicatie geheim te houden. De communicatie is slechts tijdens het transport beschermd. Alles wat buiten de sfeer valt van de verzending en wat daaraan is toe te rekenen, blijft echter wel de bescherming van het algemene privacyrecht van artikel 10 genieten.[110]

Verkeersgegevens, met andere woorden verbindingsgegevens over het transport van de communicatie, zoals tijdstippen, locatiegegevens, telefoonnummers en IP-adressen, vallen buiten de bescherming van het telefoon- en telegraafgeheim.[111] Verkeersgegevens worden wel beschermd door artikel 10 van de Grondwet voor zover zij aangemerkt kunnen worden als persoonsgegevens.[112]

---

[108] *Weber en Saravia t. Duitsland*, § 106; *Uzun t. Turkije*, § 61-63; *Shimovolos t. Rusland*, § 68.
[109] *Klass e.a. t. Duitsland*, § 52; *Association "21 Decembre 1989" e.a. t. Roemenië*, § 121.
[110] *Kamerstukken II* 1975/76, 13 872, nrs. 1-5.
[111] *Kamerstukken II* 1975/76, 13 872, nr. 3, p. 45; Rapport Staatscommissie Grondwet, 2010, p. 89, te raadplegen op www.rijksoverheid.nl.
[112] *Kamerstukken II* 1975/76, 13 872, nr. 3, p. 41-42.

Voor de vraag wanneer een verkeersgegeven een persoonsgegeven is, bieden de Wet bescherming persoonsgegevens (Wbp) en de wetsgeschiedenis enkele aanknopingspunten. Persoonsgegevens zijn alle gegevens die informatie kunnen verschaffen over een geïdentificeerde of identificeerbare natuurlijke persoon.[113] Van identificeerbaarheid is sprake wanneer de identiteit van een persoon redelijkerwijs, zonder onevenredige inspanning, kan worden vastgesteld. Hierbij spelen naast de aard van de gegevens de mogelijkheden (middelen) van de verantwoordelijke om identificatie tot stand te brengen een rol.[114] Of gegevens informatie over een persoon bevatten kan blijken uit de aard van de gegevens (bijv. feitelijke of waarderende gegevens over eigenschappen, opvattingen of gedragingen) of anders uit de context waarin de gegevens worden vastgelegd en gebruikt. Bij dit laatste is van belang of de gegevens mede bepalend zijn voor de wijze waarop de betrokken persoon in het maatschappelijk verkeer wordt beoordeeld of behandeld. Het (maatschappelijk) gebruik dat van de gegevens wordt gemaakt is dus mede bepalend voor de beantwoording van de vraag of sprake is van persoonsgegevens.[115] Volgens de memorie van toelichting bij de Wbp kunnen telefoonnummers onder omstandigheden persoonsgegevens zijn.[116] Ook het EHRM heeft in zijn jurisprudentie bepaald dat verkeersgegevens onderdeel kunnen uitmaken van de persoonlijke levenssfeer (zie nader paragraaf II.2.1).

Hoewel er al sinds 1997 discussie rond de reikwijdte en interpretatie van artikel 13 Grondwet wordt gevoerd, kan uit de wetsgeschiedenis niet anders opgemaakt worden dan dat het huidige artikel vooralsnog alleen bescherming biedt aan communicatie tijdens de transportfase.[117] In 2010 kwam de Staatscommissie Grondwet, ingesteld bij Koninklijk Besluit van 3 juli 2009, met een rapport[118] waarin onder meer aanbevolen werd artikel 13 Grondwet te wijzigen. Het Kabinet gaf aan dit advies over te nemen.[119] Vanaf 1 oktober 2012 tot 1 januari 2013 heeft het voorstel tot wijziging van artikel 13 Grondwet ter consultatie voorgelegen. De tekst van het wetsvoorstel luidt:

Artikel 13 Grondwet (wetsvoorstel)

1. Ieder heeft recht op eerbiediging van zijn brief- en telecommunicatiegeheim.
2. Beperking van dit recht is mogelijk in de gevallen bij de wet bepaald met machtiging van de rechter of, in het belang van de nationale veiligheid, met machtiging van een of meer bij de wet aangewezen ministers.
3. De wet stelt regels ter bescherming van het brief- en telecommunicatiegeheim.

Een aantal wijzigingen wordt hieronder benoemd:
Het voorstel bevat een verruiming van de reikwijdte van artikel 13 tot alle (privé of besloten) telecommunicatie, ongeacht het middel of de techniek die is gebruikt om te communiceren: e-mail, communicatie via *social media*, opslag van persoonlijke bestanden in de *cloud* en de zoekvraag om informatie op internet via een zoekmachine verkrijgen ook bescherming onder artikel 13 Grondwet.[120] Het telecommunicatiegeheim in de zin van artikel 13 ziet op een uitleg van het begrip telecommunicatie die ruimer is dan alleen elektronische communicatie, zoals gebruikt wordt in nationale en Europese regelgeving, waardoor het aantal communicatiemiddelen waarover de bescherming van artikel 13 zich uitstrekt wordt

[113] *Kamerstukken II* 1997/98, 25 892, nr. 2, p. 45.
[114] *Idem*, p. 47-50.
[115] *Idem*, p. 46.
[116] *Idem*, p. 46-47; *Kamerstukken II*, 1998/99, 25 892, nr. 6, p. 27.
[117] *Kamerstukken II* 1975/76, 13 872, nr. 3, p. 39.
[118] Rapport Staatscommissie Grondwet, 2010, te raadplegen op www.rijksoverheid.nl.
[119] *Kamerstukken II* 2011/2012, 31 570, nr. 20, p. 8.
[120] *Ontwerp toelichting Wetsvoorstel Wijziging artikel 13 Grondwet*, versie 1 oktober 2012, p. 8.

uitgebreid naar alle huidige en toekomstige (eventueel niet-elektronische) communicatiemiddelen.[121]

Het voorstel ziet niet alleen op bescherming van het transport van informatie maar ook op de tussentijdse opslag van informatie. Zo strekt de bescherming van artikel 13 zich uit tot berichten die opgeslagen zijn in een voicemail-box van een telecomprovider of in een mailbox van een e-maildienst als Gmail.[122] Maatgevend is dat zolang de derde het bericht beheert en toegang heeft tot de inhoud ervan, de bescherming van het brief- en telecommunicatiegeheim dient te gelden. [123]

Om van brief- en telecommunicatiegeheim te kunnen spreken wordt aan drie cumulatieve voorwaarden getoetst: (1) het gebruik van een *communicatiemiddel* in het communicatieproces, (2) de aanwezigheid van *een derde* die is belast met het beheer over de overdracht en/of opslag van de communicatie en tot slot (3) de noodzaak van de *gerichtheid*[124] van de communicatie.[125] Als aan deze voorwaarden is voldaan, wordt de inhoud van het bericht steeds door het brief- en telecommunicatiegeheim beschermd, ongeacht of de verzender van het bericht dit nu zo bedoeld heeft of niet.[126]

Verkeersgegevens, dat wil zeggen gegevens die ontstaan bij communicatie via daartoe bestemde kanalen, zien op de communicatie in plaats van op de inhoud van de gecommuniceerde boodschap, bijvoorbeeld op het tijdstip, plaats, duur van en betrokken nummers bij een telefoongesprek en op tijdstip, adressering en omvang van een e-mailbericht.[127] In de memorie van toelichting bij het wetsvoorstel wordt erkend dat verkeersgegevens wel zicht geven op aspecten die verband kunnen houden met de inhoud van de communicatie. Bovendien kunnen verkeersgegevens naar hun aard raken aan de telecommunicatievrijheid, in de zin dat een burger kan afzien van het voeren van bepaalde gesprekken indien hij weet of vermoedt dat de overheid weet welke telefoongesprekken hij voert. Dit doorbreekt niet de vertrouwelijkheid van de communicatie op zichzelf, maar raakt wel de vrijheid van de (tele)communicatie. Desondanks zijn verkeersgegevens niet binnen de reikwijdte van artikel 13 Grondwet gebracht, omdat zo wordt geredeneerd dat deze gegevens niet de inhoud van de telecommunicatie betreffen en een andersluidende keuze tot gevolg zou hebben dat voor inzage in verkeersgegevens steeds een rechterlijke machtiging nodig zou zijn, wat gelet op de aard van deze gegevens te vergaand zou zijn.[128] Voor zover verkeersgegevens tevens persoonsgegevens zijn, vallen deze wel onder de bescherming van artikel 10 Grondwet. In het wetsvoorstel wordt onderkend dat de inhoud van telecommunicatie soms in technische zin ook als een verkeersgegeven wordt gezien, bijvoorbeeld een sms-bericht of het onderwerp van een e-mailbericht. Hierbij luidt de conclusie dat aan de bescherming van artikel 13 Grondwet niet kan afdoen dat gegevens die de inhoud van de telecommunicatie betreffen in technische zin als een verkeersgegeven

---

[121] *Idem*, p. 8/11.
[122] *Idem*, p. 11.
[123] *Idem*, p. 14.
[124] Met gerichtheid wordt bedoeld dat de communicatie gericht moet zijn aan één of meer specifieke ontvangers. De inhoud van een bepaalde voorstelling, een openbare toespraak, informatie op het internet of *realtime audio en -video* zoals een *live* radio-uitzending of televisie zijn in beginsel geen gerichte communicatie.
[125] *Ontwerp toelichting Wetsvoorstel Wijziging artikel 13 Grondwet*, versie 1 oktober 2012, p. 12.
[126] *Idem*, p. 16.
[127] *Idem*, p. 16-17.
[128] *Idem*, p. 17.

worden beschouwd. Verkeersgegevens die niet mede betrekking hebben op de inhoud van telecommunicatie vallen echter buiten de reikwijdte van artikel 13 Grondwet.[129]

Het wetsvoorstel stelt dat beperking slechts mogelijk is in de gevallen bij wet bepaald, met machtiging van de rechter of, in het belang van de nationale veiligheid, met machtiging van een of meer bij de wet aangewezen ministers. Uit de memorie van toelichting bij het wetsvoorstel blijkt voorts dat er binnen deze systematiek wel ruimte is voor het geven van een machtiging namens de betreffende minister, door middel van mandaat. Dit mandaat wordt uitgeoefend namens, onder verantwoordelijkheid en onder aansturing van de minister.[130]

De openbare consultatie van het wetsvoorstel is afgerond op 1 januari 2013. Het wetsvoorstel is thans voor advies in behandeling bij de Raad van State. De regering heeft toegezegd het wetsvoorstel in de eerste helft van 2014 in te dienen.[131]

III Waarborgen in de Wiv 2002

Ter uitvoering van de aan de diensten opgedragen taken in het belang van de nationale veiligheid[132] beschikken de diensten over een aantal in de wet vastgelegde bevoegdheden die hen in staat stellen gegevens te verwerken. Het verwerken van (persoons)gegevens, in het bijzonder de verzameling en eventuele uitwisseling ervan, kan in meer of mindere mate inbreuk maken op de persoonlijke levenssfeer van burgers. De gradaties van de inmenging komen tot uitdrukking in de wettelijke regeling en de waarborgen die daarin zijn opgenomen ter bescherming van het privéleven van burgers. Hierbij heeft de wetgever ook in ogenschouw genomen dat de activiteiten van de diensten vanuit effectiviteitsoogpunt meestal in het geheim plaatsvinden waardoor de burger van de inmenging in zijn grondrechten in het ongewisse blijft. Teneinde het belang van de nationale veiligheid en dat van de persoonlijke levenssfeer te balanceren voorziet de Wiv 2002 in een geheel van procedures, voorwaarden en waarborgen bij de inzet van (bijzondere) bevoegdheden die zwaarder worden al naar gelang het inbreukmakende karakter van een (bijzondere) bevoegdheid van de diensten op de persoonlijke levenssfeer van burgers groter wordt. Hieronder worden de belangrijkste mechanismen die als waarborg voor de bescherming van de persoonlijke levenssfeer in de Wiv 2002 zijn opgenomen, nader besproken.

---

[129] *Ontwerp toelichting Wetsvoorstel Wijziging artikel 13 Grondwet*, versie 1 oktober 2012, p. 18.

[130] *Idem*, p. 22.

[131] *Nationaal actieplan mensenrechten, bescherming en bevordering van mensenrechten op nationaal niveau*, ministerie van Binnenlandse Zaken en Koninkrijksrelaties, december 2013, p. 17, te raadplegen via www.rijksoverheid.nl.

[132] *Taken van de AIVD* (artikel 6 lid 2 Wiv 2002): onderzoek naar (potentiële) dreiging ten aanzien van Nederland of Nederlandse belangen (a-taak), veiligheidsonderzoeken (b-taak), veiligheidsbevorderende maatregelen (c-taak), onderzoek naar bepaalde landen ter ondersteuning van de regering met politieke inlichtingen (d-taak), dreigings- en risicoanalyses in het kader van het stelsel bewaken en beveiligen (e-taak). *Taken van de MIVD* (artikel 7 lid 2 Wiv 2002): onderzoek ten behoeve van de uitvoering van internationale crisisbeheersings- en vredesoperaties (a-taak), veiligheidsonderzoeken (b-taak), onderzoek in het kader van contra-inlichtingen en veiligheid ten aanzien van de krijgsmacht (c-taak), veiligheidsbevorderende maatregelen (d-taak), onderzoek naar bepaalde landen met een militaire relevantie ter ondersteuning van de regering met politieke inlichtingen (e-taak), dreigingsanalyses in het kader van het stelsel bewaken en beveiligen (f-taak).

Het noodzakelijkheidsvereiste uit artikel 8 EVRM is op meerdere plaatsen in de Wiv 2002 opgenomen. Allereerst in artikel 12 Wiv 2002 dat betrekking heeft op alle gegevensverwerkende activiteiten van de diensten. In het artikel is verwoord dat de diensten slechts gegevens mogen verwerken indien dit plaatsvindt voor een bepaald doel en slechts voor zover dat noodzakelijk is voor een goede uitvoering van de Wiv 2002 of de Wvo. Met de zinsnede "goede uitvoering van de Wiv 2002 of de Wvo" wordt bedoeld dat de verwerking van gegevens door de diensten primair gerelateerd dient te zijn aan de uitvoering van de aan hen opgedragen taken – dus in het belang van de nationale veiligheid – en de daaraan gerelateerde beheersfuncties (zoals personeels- en salarisadministratie), maar dat ook ruimte wordt gelaten voor andere – bij of krachtens de Wiv 2002 of Wvo – voorziene verwerkingen, zoals het verstrekken van gegevens in het kader van de uitoefening van het recht op kennisneming en samenwerking met buitenlandse diensten.[133] Daarnaast is het noodzakelijkheidsvereiste voor de toepassing van bijzondere bevoegdheden opgenomen in artikel 18 Wiv 2002. Hierin is bepaald dat bijzondere bevoegdheden enkel mogen worden ingezet indien dit noodzakelijk is voor de uitvoering van bepaalde taken van de diensten.[134] Het werd door de wetgever niet noodzakelijk, laat staan wenselijk, geacht dat de diensten bij elke taak bijzondere bevoegdheden kunnen toepassen. De beperking tot bepaalde taakgebieden hangt nauw samen met de aanzienlijke inbreuk op de persoonlijke levenssfeer van burgers die met bijzondere bevoegdheden kan worden gemaakt. Voor de taken waarbij bijzondere bevoegdheden niet zijn toegestaan, voldoet de algemene bevoegdheid tot het verzamelen van gegevens als bedoeld in artikel 17 Wiv 2002.[135] Het noodzakelijkheidsvereiste voor de inzet van bijzondere bevoegdheden, komt behalve in artikel 18, ook terug in artikel 32 Wiv 2002. Hierin wordt bepaald dat de inzet van bijzondere bevoegdheden gestaakt dient te worden als het daarmee beoogde doel is bereikt, met andere woorden als de inzet niet langer noodzakelijk is met het oog op het nagestreefde doel. Het spreekt voor zich dat als het middel niet (meer) bijdraagt of bij kan dragen aan het doel, het middel dan eveneens niet (langer) ingezet mag worden. Dit betekent dat de diensten voorafgaande aan de inzet van een bijzondere bevoegdheid een doel dienen te hebben waarvoor het middel wordt ingezet en dat de verwachting dient te bestaan dat de opbrengst van de inzet van het middel bijdraagt aan het bereiken van dat doel. Na aanvang van de inzet zal de opbrengst ook daadwerkelijk moeten bijdragen aan het onderzoek om de inzet te kunnen continueren.

Aangezien de uitoefening van bijzondere bevoegdheden diep in de persoonlijke levenssfeer van burgers kan ingrijpen, heeft de wetgever daarvoor een aantal strikte waarborgen ingebouwd, zoals een limitatieve opsomming van de toegestane inlichtingenmiddelen, het toestemmingsvereiste, een limiet aan de duur van de inzet van de bijzondere bevoegdheid en de vereisten van noodzakelijkheid (hierboven al aan de orde gesteld), proportionaliteit en subsidiariteit bij de inzet ervan.

In het pakket aan bijzondere bevoegdheden dat de AIVD en de MIVD ter beschikking staat valt niet zonder meer een hiërarchische structuur aan te brengen naar de mate van inbreuk voor de betrokkene. Uit de door de wetgever aangebrachte gradaties in de toestemming die moet worden gegeven voor de inzet van een inlichtingenmiddel, kan worden afgeleid dat een hoger toestemmingsniveau een zwaardere inbreuk op de rechten van betrokken personen inhoudt dan een lager niveau. Dit zegt echter niet alles. In de praktijk wordt de zwaarte van de inbreuk toch vooral bepaald door de technische en praktische invulling van

[133] *Kamerstukken II* 1997/98, 25 877, nr. 3, p. 18.
[134] Voor de AIVD gaat het om de a- en de d-taak. Voor de MIVD om de a-, c- en e-taak.
[135] *Kamerstukken II* 1997/98, 25 877, nr. 3, p. 26.

een bijzondere bevoegdheid en de duur en opbrengst van de inzet.[136] Wordt een telefoon bijvoorbeeld slechts voor een dag afgeluisterd, wordt een frequentie slechts kort geïntercepteerd of levert de selectie van ongerichte interceptie geen enkele treffer op, dan is de daadwerkelijke inbreuk minder groot dan wanneer een van de diensten gedurende een jaar iedere maand de telefonieverkeersgegevens van een persoon opvraagt. Dit neemt overigens niet weg dat ook indien de inzet van de bijzondere bevoegdheid slechts korte tijd plaatsvindt en de opbrengst nihil is, er wel degelijk een inbreuk wordt gemaakt.[137] Per geval zal dan ook van tevoren moeten worden beoordeeld hoe zwaar de verwachte inbreuk is en of wordt voldaan aan de voorwaarden van proportionaliteit en subsidiariteit. Dit dient duidelijk terug te komen in de motivering voor de inzet van een bijzondere bevoegdheid. Bij de totstandkoming van de Wiv 2002 zijn deze toetsingscriteria uit het EVRM en de jurisprudentie van het EHRM (zie paragraaf II.2) in de artikelen 31 en 32 Wiv 2002 opgenomen. Het vereiste van proportionaliteit (artikel 31 Wiv 2002) houdt in dat de uitoefening van een bevoegdheid in een evenredige verhouding dient te staan tot het daarmee beoogde doel (lid 4) en achterwege dient te blijven, indien de uitoefening ervan voor betrokkene een onevenredig nadeel in vergelijking tot het nagestreefde doel oplevert (lid 3). Dit houdt in dat een afweging dient plaats te vinden tussen het belang dat met de inzet van de bijzondere bevoegdheid wordt gediend (de nationale veiligheid) en de belangen van de betrokkene (het recht op eerbiediging van de persoonlijke levenssfeer).[138] Tevens dient de inmenging zo licht mogelijk te zijn, ook wel bekend als het subsidiariteitsvereiste (artikel 31 leden 1 en 2 en artikel 32 Wiv 2002). Dit bekent dat een bijzondere bevoegdheid pas mag worden ingezet indien de daarmee beoogde verzameling van gegevens niet of niet tijdig op andere wijze, zonder de inzet van een bijzondere bevoegdheid, kan plaatsvinden (artikel 31 lid 1 Wiv 2002).[139] Ook dient slechts die bevoegdheid te worden uitgeoefend, die gelet op de omstandigheden van het geval, waaronder de ernst van de bedreiging van de door een dienst te beschermen belangen, mede in vergelijking met andere beschikbare bevoegdheden, voor de betrokkene het minste nadeel oplevert (artikel 31 lid 2 Wiv 2002). Een bijzondere bevoegdheid dient bovendien te worden gestaakt indien met de uitoefening van een minder ingrijpende bevoegdheid kan worden volstaan (artikel 32 Wiv 2002).

Met het oog op de persoonlijke levenssfeer van burgers voorziet de wet in een gradatie van handelingen op het gebied van gegevensverzameling. Hiermee wordt uiting gegeven aan het subsidiariteitsvereiste. De diensten dienen eerst gebruik te maken van de minst inbreukmakende bevoegdheden (algemene bevoegdheid) en daarna, indien dat noodzakelijk blijkt, pas op te schalen naar meer inbreukmakende bevoegdheden (bijzondere bevoegdheden). Concreet bestaat dit eerst uit het raadplegen van eigen bestanden (informatie die de diensten al in huis hebben), vervolgens indien noodzakelijk het raadplegen van voor een ieder toegankelijke – open – informatiebronnen, zoals internet, of informatiebronnen waarvoor de diensten een recht op kennisneming van de daar berustende informatie hebben, zoals de Gemeentelijke basisadministratie persoonsgegevens (GBA) of politieregisters, dan wel het bevragen van informanten (artikel 17 Wiv 2002) en ten slotte,

---

136 *Kamerstukken II* 1997/98, 25 877, nr. 3, p. 29.

137 Toezichtsrapport van de CTIVD nr. 28 inzake de inzet van Sigint door de MIVD, *Kamerstukken II* 2011/12, 29 924, nr. 74 (bijlage), paragraaf 5.2, beschikbaar op www.ctivd.nl.

138 Afhankelijk van welke bijzondere bevoegdheid wordt ingezet en de maatschappelijke positie die een persoon of een organisatie tegen wie de bevoegdheid wordt ingezet inneemt, kunnen de belangen ook andere rechten omvatten, zoals het telefoongeheim (artikel 13 Grondwet), het verschoningsrecht voor advocaten en andere geheimhouders, het bronbeschermingsrecht voor journalisten of diplomatieke onschendbaarheid.

139 *Kamerstukken II* 1997/98, 25 877, nr. 3, p. 52.

voor zover de wet in deze mogelijkheid voorziet en dit noodzakelijk blijkt, de inzet van bijzondere inlichtingenmiddelen (artikelen 18 e.v. Wiv 2002)[140], waarbij er rekenschap van wordt gegeven dat het inbreukmakende karakter van de bijzondere bevoegdheden onderling verschillend is en dat voor de minst mogelijke inmenging wordt gekozen.

Een belangrijke waarborg voor de bescherming van het privéleven van individuen is het vereiste van toestemming voor de toepassing van bijzondere bevoegdheden. Het toestemmingsniveau is niet voor alle bijzondere bevoegdheden hetzelfde. In de regel dient de betrokken minister of namens deze het hoofd van een dienst toestemming te geven, tenzij de desbetreffende bepaling anders stelt (artikel 19 lid 1 Wiv 2002). Het hoofd van een dienst kan de bevoegdheid om toestemming te geven weer verder mandateren (artikel 19 lid 2 Wiv 2002). In een aantal gevallen heeft de wet expliciet bepaald dat alleen de betrokken minister toestemming kan geven. Dit hangt samen met de bescherming van het telefoon- en telegraafgeheim door artikel 13 van de Grondwet.[141] Hiervan is sprake – voor zover relevant voor dit onderzoek – bij een tap (artikel 25 Wiv 2002) en de selectie van ongericht ontvangen en opgenomen niet-kabelgebonden telecommunicatie (artikel 27 leden 3 en 4 Wiv 2002). Voor andere bevoegdheden kan het toestemmingsniveau bij het hoofd van de dienst zijn gebleven of door submandatering op een lager ambtelijk niveau zijn toegestaan. Voor de AIVD is toestemming voor de inzet van een agent (artikel 21 Wiv 2002) en voor hacken (artikel 24 Wiv 2002) ingevolge het Mandaatbesluit bijzondere bevoegdheden AIVD 2009 toebedeeld aan de directeur van de eenheid respectievelijk het unithoofd.[142] Voor de MIVD is bepaald dat de inzet van een agent en het hacken van een geautomatiseerd werk niet worden gemandateerd aan het hoofd van de dienst voor zover het de eerste aanvraag betreft, waarvoor dus toestemming aan de minister van Defensie moet worden gevraagd.[143] Een formele toestemmingsprocedure ontbreekt volgens de wet voor het opvragen van telefonieverkeersgegevens (artikel 28 Wiv 2002)[144] en het opvragen van abonneegegevens (artikel 29 Wiv 2002), omdat dit geen inhoudelijk verkeer betreft, alsook voor *searchen* (artikel 26 lid 2 Wiv 2002) en ongerichte interceptie (artikel 27 lid 2 Wiv 2002), omdat hierbij nog geen kennis van de inhoud van de informatie wordt genomen, en voor militair berichtenverkeer (artikel 25 lid 8 Wiv 2002) omdat dit nauwelijks het privéleven raakt. In bepaalde gevallen[145] dient de toestemming door de minister van Defensie te worden verleend in overeenstemming met de minister van BZK indien de inzet van de bijzondere bevoegdheid plaatsvindt op een plaats die niet in het gebruik is bij het ministerie van Defensie.[146] Dit om een ongewenste interferentie met onderzoeken van de AIVD te voorkomen. Met het vereiste van toestemming hangt samen dat een bijzondere bevoegdheid na het verkrijgen van de benodigde toestemming niet onbeperkt kan worden uitgeoefend. Ook in de limitering van de duur van de uitoefening schuilt een belangrijke waarborg voor de bescherming van het privéleven van burgers. In beginsel geldt de inzet van een

[140] *Kamerstukken II* 2000/01, 25 877, nr. 59, p. 4-5.

[141] In het wetsvoorstel ter wijziging van artikel 13 Grondwet wordt voorgesteld om, in geval van beperkingen in het belang van de nationale veiligheid, het verlenen van toestemming door de minister tot uitgangspunt te nemen, maar uitdrukkelijk mandatering toe te staan; *Ontwerp toelichting Wetsvoorstel Wijziging artikel 13 Grondwet*, versie 1 oktober 2012, p. 22.

[142] Mandaatbesluit bijzondere bevoegdheden AIVD 2009, artikel 4 (agent), artikel 7 (hacken).

[143] Mandaatregeling Defensie Wet op de inlichtingen- en veiligheidsdiensten 2002 en Wet veiligheidsonderzoeken, *Stcrt.* 2002, 147.

[144] Hierbij dient te worden opgemerkt dat het verzoek om de verkeersgegevens ingevolge artikel 28, vierde lid, Wiv 2002 dient te worden gedaan door het hoofd van de dienst.

[145] In het kader van dit onderzoek is van belang: Artikel 24, tweede lid; artikel 25, derde lid; artikel 27, achtste lid; en artikel 28, vijfde lid.

[146] *Kamerstukken II* 1999/2000, 25 877, nr. 8, p. 17.

bijzondere bevoegdheid voor een periode van ten hoogste drie maanden, tenzij de wet anders bepaalt, waarna op verzoek telkens verlenging voor eenzelfde periode mogelijk is (artikel 19 lid 3 Wiv 2002).

IV Gegevensverwerking door de diensten

IV.1 Algemeen kader voor gegevensverwerking

De Wiv 2002 stelt een aantal algemene voorwaarden voor de verwerking van gegevens door de diensten. Deze eisen gelden ten aanzien van alle vormen van gegevensverwerking. In artikel 12 Wiv 2002 is de algemene bevoegdheid van de diensten om gegevens te verwerken vastgelegd. Het gaat hierbij om de verwerking van zowel persoonsgegevens als van andere gegevens. Uitdrukkelijk is opgenomen dat de diensten zich bij de verwerking van gegevens dienen te houden aan de eisen die daaraan bij of krachtens de Wiv 2002 of de Wet veiligheidsonderzoeken (Wvo) zijn gesteld. De regeling voor de verwerking van gegevens in de Wiv 2002 is uitputtend. De Wet bescherming persoonsgegevens (Wbp) is expliciet niet van toepassing (artikel 2 Wbp). Wel is voor de regeling in de Wiv 2002 op verschillende punten aangesloten bij wat in de Wbp is bepaald, zoals bij de definitie van gegevensverwerking en de algemene eisen die aan gegevensverwerking worden gesteld. Deze eisen vormen weer een uitdrukking van de in het privacyrecht en de over artikel 8 EVRM ontwikkelde algemene beginselen van onder meer proportionaliteit en subsidiariteit.

Gegevensverwerking dient te voldoen aan een aantal algemene eisen, opgenomen in de artikelen 12, 13, 15 en 16 van de Wiv 2002. Zo mag de verwerking van gegevens slechts plaatsvinden voor een bepaald doel en voor zover dat noodzakelijk is voor een goede uitvoering van de Wiv 2002 of de Wvo (artikel 12 lid 2 Wiv 2002). Het noodzakelijkheidsvereiste is in paragraaf III besproken. Het vereiste van doelbinding impliceert een voldoende gespecificeerd doel dat intern is vastgelegd. Gegevens die, gelet op het doel waarvoor zij worden verwerkt hun betekenis hebben verloren dienen te worden verwijderd en vernietigd met inachtneming van het bepaalde in de artikelen 43 en 44 Wiv 2002. Voorts dient de verwerking van gegevens in overeenstemming met de wet en op een behoorlijke en zorgvuldige wijze plaats te vinden (artikel 12 lid 3 Wiv 2002). Het algemene vereiste dat gegevensverwerking op een behoorlijke wijze dient te geschieden biedt een aanknopingspunt voor een proportionaliteitsvereiste, zoals artikel 8 EVRM vereist, bij alle vormen van gegevensverwerking, aangezien evenredigheid van het middel ten opzichte van het doel één van de normen is van behoorlijk overheidsoptreden. Behoorlijk overheidsoptreden houdt bovendien in dat de overheid de grondrechten van haar burgers respecteert, hetgeen betekent dat de diensten bij het verwerken van (persoons)gegevens rekening moeten houden met de inbreuk die hierdoor wordt gemaakt op het privacyrecht en eventuele andere rechten van de betrokkene.[147] Verder dienen verwerkte gegevens te zijn voorzien van een aanduiding over de mate van betrouwbaarheid dan wel een verwijzing naar het document of de bron waaraan de gegevens zijn ontleend (artikel 12 lid 4 Wiv 2002). In artikel 13 Wiv 2002 is limitatief neergelegd ten aanzien van welke categorieën van personen de gegevensverwerking kan plaatsvinden. De artikelen 15 en 16 Wiv 2002 betreffen een aantal zorgplichten, die binnen de diensten in de praktijk een nadere uitwerking hebben gekregen. Zo dienen de diensten zorg te dragen voor geheimhouding van daarvoor in aanmerking komende bronnen waaruit gegevens afkomstig zijn (artikel 15, aanhef en onder

[147] Zie voor de algemene behoorlijkheidsnormen: De Nationale ombudsman, 'Behoorlijkheidswijzer', 2012, te raadplegen via www.nationaleombudsman.nl.

b Wiv 2002) en voor de veiligheid van de personen met wier medewerking gegevens worden verzameld (artikel 15, onder c, Wiv 2002). Op grond van artikel 16 Wiv 2002 – dat vooral betrekking heeft op de technische en organisatorische inrichting van de gegevensverwerking – dienen de diensten zorg te dragen voor de juistheid en volledigheid van de gegevens, voor voorzieningen ter beveiliging van de gegevens en voor limitering van de toegang tot de gegevens. Dit laatste vormt samen met artikel 35 Wiv 2002, waarin het *need to know*-principe is vastgelegd, de basis voor het autorisatie- en authentificatiebeleid binnen de diensten voor toegang tot informatiesystemen en daarin opgenomen gegevens(bestanden). Het *need to know*-principe stelt de norm voor interne verstrekking van gegevens. Interne verstrekking van gegevens dient slechts plaats te vinden voor zover dat noodzakelijk is voor een goede uitvoering van de aan de desbetreffende ambtenaar[148] opgedragen taak.

IV.2 Verwerking van gegevensverzamelingen

Bij verwerking van gegevens gaat het niet alleen om gegevens over specifieke personen of organisaties waarin de diensten op grond van hun taken belangstelling hebben, maar kan het ook gaan om verzamelingen van gegevens (gegevensverzamelingen). Gegevensverzamelingen kunnen binnen de diensten ontstaan door het samenbrengen van verwerkte gegevens, maar kunnen ook verkregen worden uit open bronnen, door het op grond van vrijwilligheid bevragen van externe partijen (overheid, bedrijfsleven of andere partijen die steeds vaker de beschikking hebben over geautomatiseerde gegevensverzamelingen), door inzet van een bijzondere bevoegdheid (bijvoorbeeld door ongerichte interceptie of door hacken) of door samenwerking met buitenlandse inlichtingen- en/of veiligheidsdiensten. Ook kunnen de diensten onder omstandigheden rechtstreeks toegang (op afstand) tot bepaalde gegevensverzamelingen hebben. In de paragrafen IV en V wordt nader ingegaan op het verzamelen van gegeven door de diensten. Door middel van (geautomatiseerde) gegevensverzamelingen kunnen de diensten over een grote(re) hoeveelheid voor hun taakuitvoering relevante gegevens de beschikking krijgen. Omdat deze gegevensverzamelingen ook gegevens bevatten van personen die vanuit de taakstelling van de diensten geen aandacht hebben en de bestanden vaak vormen van data-analyse vereisen voorafgaande aan verder intern gebruik, doet de verwerking van dergelijke gegevensverzamelingen vragen rijzen over de juridische grondslag daarvan in de Wiv 2002.

De Wiv 2002 spreekt in artikel 1 over "gegevens" waarmee gedoeld wordt op persoonsgegevens en andere gegevens. In de wet noch in de wetsgeschiedenis wordt expliciet gesproken over gegevensverzamelingen, maar niet valt in te zien waarom verzamelingen van (persoons)gegevens niet onder het begrip gegevens zouden vallen. Dit houdt in dat het algemene kader voor gegevensverwerking, zoals vastgelegd in de artikelen 12 t/m 16 Wiv 2002, ook geldt voor verwerking van gegevensverzamelingen. Hier verdient artikel 13 Wiv 2002 in het bijzonder vermelding omdat daarin uitputtend is geregeld ten aanzien van welke (categorieën van) personen verwerking van gegevens mag plaatsvinden. Hierbij wordt primair aansluiting gezocht bij de taakstellingen van de diensten in de artikelen 6 (AIVD) en 7 (MIVD). Voor beide diensten voorziet artikel 13 Wiv 2002 in een categorie van personen "wier gegevens noodzakelijk zijn ter ondersteuning van een goede taakuitvoering door de dienst" (lid 1 onder e (AIVD) en lid 2 onder e (MIVD)). In deze categorie kan een juridische grondslag worden gezien voor de verwerking van gegevens van personen in (geautomatiseerde) gegevensverzamelingen die geen aandacht vanuit de taakstelling van de diensten genieten. Voor wat betreft de toelaatbaarheid van data-analyse als (geautomatiseerde) gegevensverwerking biedt artikel 1 Wiv 2002, waarin het begrip

[148] Werkzaam binnen een van de diensten of voor de diensten op grond van artikel 60 Wiv 2002.

gegevensverwerking is uitgewerkt, de juridische basis in combinatie met artikel 12 lid 1 Wiv 2002. Onder gegevensverwerking wordt ook gerekend het samenbrengen alsmede het met elkaar in verband brengen van gegevens, wat twee vormen van data-analyse zijn. Voorts dient volgens de wetsgeschiedenis onder gegevensverwerking zowel handmatige als geautomatiseerde verwerking te worden verstaan.[149]

Hoewel gesteld kan worden dat de Wiv 2002 een voldoende basis biedt voor (geautomatiseerde) verwerking van verzamelingen gegevens, voorziet de wet niet in expliciete bepalingen daaromtrent. In verband met een toegenomen gebruik van deze werkwijze door de diensten in de afgelopen jaren dient de vraag zich aan of de grondslag in de huidige Wiv 2002 op dit punt nog steeds voldoende is.

In het zogenoemde post-Madridwetsvoorstel[150], dat uiteindelijk werd ingetrokken, was hiervoor een voorziening opgenomen, met name om tegemoet te komen aan de publieke bezorgdheid en onduidelijkheid over dit onderwerp. Het wetsvoorstel beoogde bij te dragen aan het effectiever en efficiënter functioneren van de diensten, mede in het licht van de aanslagen in New York, Madrid en Londen en de aanslag op Van Gogh. In de memorie van toelichting bij het wetsvoorstel werd aangegeven dat bij de uitvoering van de Wiv 2002 onder andere was gebleken dat de wet in een aantal gevallen onvoldoende expliciet was waar het de (mogelijkheden tot) toepassing van bepaalde methodieken voor gegevensverwerking, zoals data-analyse, en de mogelijkheden tot het verkrijgen (c.q. verlenen) van rechtstreekse toegang tot bepaalde gegevensverzamelingen betrof.[151] Volgens de memorie van toelichting bij het wetsvoorstel was data-analyse een gangbare werkmethode bij de diensten die verschillende verschijningsvormen had en die door de ontwikkelingen in de informatietechnologie steeds meer mogelijkheden bood. In het voorgestelde artikel 12a werd data-analyse als werkmethode door de diensten geëxpliciteerd door aan te geven dat tot vormen van data-analyse die de diensten (kunnen) toepassen worden gerekend het doorzoeken van gegevens aan de hand van profielen of het vergelijken van gegevens met het oog op patronen. Ten behoeve van deze vormen van data-analyse maakten de diensten volgens de memorie van toelichting gebruik van gegevens in eigen geautomatiseerde gegevensverzamelingen, maar ook van gegevens die waren opgenomen in geautomatiseerde gegevensverzamelingen die bij derden voorhanden zijn en die op vrijwillige basis (al dan niet onder toepassing van artikel 17 Wiv 2002) aan de diensten beschikbaar waren gesteld.[152] Hoewel data-analyse volgens de memorie van toelichting bij het wetsvoorstel dus al tot de gereedschapskist van de diensten behoorde en ook al een deugdelijke wettelijke grondslag kende, werd het niettemin wenselijk geacht om deze op onderdelen explicieter wettelijk te normeren teneinde hierdoor de kenbaarheid te vergroten en de toepassing ervan op onderdelen met extra waarborgen te omgeven.[153]

De aanpassing van de Wiv 2002 voorzag ook in een aanpassing van artikel 13 Wiv 2002 vanwege de in de praktijk ondervonden onduidelijkheid over de uitleg van het huidige eerste en tweede lid, onder e, in relatie tot de werkwijze van data-analyse als

---

[149] *Kamerstukken II* 1997/98, 25 877, nr. 3, p. 17.

[150] Wijziging van de Wet op de Inlichtingen- en Veiligheidsdiensten 2002 in verband met de verbetering van de mogelijkheden van de inlichtingen- en veiligheidsdiensten om onderzoek te doen naar en maatregelen te nemen tegen terroristische en andere gevaren met betrekking tot de nationale veiligheid alsmede enkele andere wijzigingen, *Kamerstukken II* 2005/06, 30 553, nr. 3.

[151] *Idem*, p. 3.

[152] *Idem.*

[153] *Idem*, p. 24-26; *Kamerstukken I* 2007/08, 30 553, C, p. 12.

gegevensverwerking. Daarom werd in een nieuw lid uitdrukkelijk opgenomen dat bij de toepassing van de twee genoemde vormen van data-analyse in het voorgestelde artikel 12a op gegevensverzamelingen van derden ook persoonsgegevens kunnen worden verwerkt van personen die niet al eerder in beeld zijn gekomen bij de dienst, maar waarvan de verwerking van gegevens, omdat deze nu eenmaal een integraal deel uitmaken van een dergelijk gegevensbestand, niettemin noodzakelijk moet worden geacht ter ondersteuning van een goede taakuitvoering van een dienst.[154] Ook werd een aanpassing voorzien van artikel 17 (in de zin dat geëxpliciteerd werd dat vrijwillige verstrekking van gegevens ook geautomatiseerde gegevensverzamelingen kan betreffen) en opname van een artikel 29b (inhoudende een verplichting tot het verstrekken van (delen van) geautomatiseerde gegevensverzamelingen door aan te wijzen bestuursorganen en categorieën van financiële dienstverleners en vervoerders).

In zijn advies op het wetsvoorstel heeft het College bescherming persoonsgegevens (CBP) onder meer aangegeven niet overtuigd te zijn van de noodzaak van de introductie van een verplichting tot verstrekking van verzamelingen gegevens voor bepaalde categorieën van personen en instellingen. Ook had het CBP twijfels bij de voorgestelde bepaling over data-analyse, omdat hiermee een grotere druk op de diensten zou komen te liggen om meer gegevens te analyseren, geen garanties bestonden over de kwaliteit van de verkregen gegevens en of daaruit getrokken conclusies overeenkwamen met de werkelijkheid, en het risico van *function creep* in de zin dat enerzijds technologieën die aanvankelijk gericht waren op een bepaalde groep van personen (die vanuit de taakstelling van de diensten aandacht behoeven) gaandeweg op (bijna) iedereen toegepast konden worden, terwijl anderzijds verzamelde gegevens voor een bepaald doel (dat van de persoon of instelling die de gegevens heeft vastgelegd) verstrekt en verwerkt zouden worden ten behoeve van een ander doel (in het belang van de nationale veiligheid).[155]

In reactie op het advies van het CBP op het wetsvoorstel benadrukte de regering onder meer dat de diensten er geenszins op gericht zijn ongebreidelde gegevensverzamelingen aan te leggen die niet relevant zijn voor de aan hen opgedragen taken. Hiertoe zijn zij ook niet bevoegd, zo wijzen onder meer de artikelen 12 en 13 Wiv 2002 uit.[156] Tevens werd benadrukt dat aan gegevensverwerking bij de diensten altijd een gerichte onderzoeksvraag ten grondslag ligt die voortvloeit uit de taakopdracht van de diensten. *Fishing expeditions* of ongerichte bestandsvergelijking is niet geoorloofd en in strijd met artikel 12 van de Wiv 2002.[157]

Het wetsvoorstel tot wijziging van de Wiv 2002 werd door de Tweede Kamer aangenomen, maar strandde, mede vanwege de kritische noten van het CBP[158], in de Eerste Kamer.[159] De regering heeft hierop in 2011 besloten om het wetsvoorstel in te trekken.[160]

De verwerking van gegevensverzamelingen dient in de huidige situatie aan de algemene eisen van gegevensverwerking (artikel 12 Wiv 2002) te voldoen, dus onder meer voor een

---

154 *Kamerstukken II* 2005/06, 30 553, nr. 3, p. 26.
155 Advies CPB van 20 december 2007, bijlage bij *Kamerstukken I* 2007/08, 30 553, B, p. 7-8/10-11.
156 *Kamerstukken I* 2007/08, 30 553, C, p. 5.
157 *Idem*, p. 8.
158 Advies CPB van 20 december 2007, bijlage bij *Kamerstukken I* 2007/08, 30 553, B; reactie CPB van 25 juni 2008 op de kabinetsreactie CPB-advies Wiv 2002 (30 553, C), bijlage bij *Kamerstukken I* 2007/08, 30 553, D.
159 *Kamerstukken I* 2008/09, 30 553, E.
160 *Kamerstukken I* 2010/11, 30 553, F; *Kamerstukken II* 2010/11, 30 553, nr. 18.

bepaald doel en slechts voor zover noodzakelijk voor een goede uitvoering van de wet. Uit het vereiste dat gegevensverwerking op een behoorlijke wijze dient te geschieden vloeit voort dat de inbreuk op de persoonlijke levenssfeer van burgers evenredig (proportioneel) dient te zijn aan het nagestreefde doel. Het vereiste dat gegevensverwerking voor een bepaald doel behoort plaats te vinden, betekent dat de diensten in het kader van gegevensverzameling niet zomaar externe gegevensverzamelingen mogen binnenhalen (of daar rechtstreeks toegang toe mogen verkrijgen) en verder verwerken. In verband met het vereiste van noodzakelijkheid dient vooraf, dus voor de daadwerkelijke verwerving, vastgesteld te worden welke gegevens noodzakelijk worden geacht voor een goede taakuitvoering. Bij het doel waarvoor het gegevensbestand wordt verworven rijst de vraag hoe specifiek dit moet zijn. Het is immers goed mogelijk dat gegevensverzamelingen – buiten een specifiek onderzoek – noodzakelijk kunnen zijn ter ondersteuning van de taakuitvoering in brede zin, dus niet alleen op een bepaald moment maar ook in de toekomst, bijvoorbeeld doordat een bestand vaker bevraagd kan worden. Het doelcriterium in de Wiv 2002 is minder strikt geformuleerd dan in de Wet bescherming persoonsgegevens (Wbp), waarin wordt bepaald dat persoonsgegevens voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld (artikel 7). Uit de ruimere formulering van het doelcriterium in de Wiv 2002 kan worden afgeleid dat verzameling van gegevensverzamelingen ook legitiem is indien dit geschied voor een breder, maar wel vooraf omschreven en gemotiveerd, doel waaruit blijkt dat de verwerking noodzakelijk is voor een goede taakuitvoering. Vervolgens dient als waarborg voor de persoonlijke levenssfeer van burgers de toegang tot de bestanden – in overeenstemming met het bepaalde in de artikelen 15, 16 en 35 Wiv 2002 – voldoende te worden beperkt. Ook de in de artikelen 43 en 44 Wiv 2002 opgenomen regels omtrent de verwijdering, vernietiging en archivering van verwerkte gegevens vormen een waarborg voor de bescherming van de persoonlijke levenssfeer van burgers.

Het gebruik van de gegevensverzamelingen dient overeenkomstig het doel waarvoor ze zijn verworven plaats te vinden. Anders dan de Wbp (artikel 9) geeft de Wiv 2002 geen nadere regels voor gebruik van gegevens(bestanden) voor andere doeleinden dan waarvoor ze zijn verworven. Op grond van de Wbp wordt een (on)verenigbaarheidseis gehanteerd inhoudende dat persoonsgegevens niet verder mogen worden verwerkt op een wijze die onverenigbaar is met de doeleinden waarvoor ze zijn verkregen, waarbij onder meer rekening wordt gehouden met het doelbindingsprincipe, wat wil zeggen dat hoe verder het oorspronkelijke doel afstaat van het latere doel des te minder sprake is van verenigbaarheid. De Wiv 2002 kent een dergelijke bepaling niet. Er wordt alleen voorzien in artikel 43 Wiv 2002 dat bepaalt dat gegevens die gelet op het doel waarvoor zij worden verwerkt hun betekenis hebben verloren, worden verwijderd. De verwijderde gegevens worden vervolgens vernietigd, tenzij wettelijke regels omtrent bewaring daaraan in de weg staan.[161]

[161] Ten aanzien van de AIVD heeft de Commissie geconstateerd dat de dienst in de praktijk geen structureel actief derubriceringsprogramma kent, zie voor een nadere bespreking van dit onderwerp het toezichtsrapport van de CTIVD nr. 33 inzake de rubricering van staatsgeheimen door de AIVD, *Kamerstukken II* 2011/12, 30 977, nr. 47 (bijlage), paragraaf 10, beschikbaar op www.ctivd.nl.

V Het verzamelen van gegevens

V.1 Algemene bevoegdheid

Artikel 17 Wiv 2002 bevat de algemene bevoegdheid van de diensten om gegevens te verzamelen. Op grond van deze algemene bevoegdheid mogen de diensten gegevens verzamelen in het kader van de uitvoering van hun taken alsmede ter ondersteuning van een goede taakuitvoering, waarbij onder meer gedoeld wordt op onderzoek gericht op het vaststellen van de betrouwbaarheid van de personen van wier diensten gebruik wordt gemaakt, bijvoorbeeld een agent van de dienst.[162] In deze bepaling is neergelegd dat de diensten zich voor gegevens kunnen wenden tot a) bestuursorganen, ambtenaren en voorts een ieder die geacht wordt de benodigde gegevens te kunnen verstrekken en b) de verantwoordelijke voor een gegevensverwerking. In beginsel worden de benodigde gegevens verzameld uit voor een ieder toegankelijke bronnen (open bronnen informatie), door raadpleging van niet-openbare gegevensverzamelingen (waarvoor aan de diensten een recht op kennisneming van de daar berustende gegevens is verleend[163]) en door raadpleging van personen en instanties die mogelijk beschikken over relevante gegevens (ook wel informanten genoemd), hieronder kunnen ook buitenlandse inlichtingen- en/of veiligheidsdiensten worden geschaard (op de samenwerking met buitenlandse diensten wordt ingegaan in paragraaf VI). Volgens het derde lid van artikel 17 Wiv 2002 kunnen eventuele bij of krachtens de wet geldende voorschriften ten aanzien van de verstrekking van de gevraagde gegevens de diensten niet worden tegengeworpen. De bepaling van het derde lid betekent echter niet dat de beoogde verstrekker volgens artikel 17 Wiv 2002 verplicht zou zijn om de gevraagde gegevens te verstrekken. Het uitgangspunt is de vrijwillige verstrekking van gegevens.

Artikel 17 Wiv 2002 betreft een ruime bevoegdheid voor de diensten. Dit is geen bijzondere bevoegdheid, hoewel het ook heimelijk geschiedt en een inbreuk kan maken op de persoonlijke levenssfeer. Op grond van deze bepaling kunnen de diensten gegevens(bestanden) verzamelen bij alle personen en instanties die geacht worden deze gegevens te kunnen verstrekken. Dat houdt in dat informanten benaderd en bevraagd kunnen worden die op basis van vrijwilligheid gegevens voor de diensten kunnen verzamelen, omdat zij daartoe bijvoorbeeld toegang hebben op grond van de functie die ze vervullen of de groepering waarin zij verkeren.[164] Een informant mag alleen worden geraadpleegd en niet worden geïnstrueerd of gestuurd.[165] Ook het verzamelen van bancaire gegevens valt onder deze algemene bevoegdheid, wat betekent dat hiervoor geen toestemming nodig is.[166] Dit is anders in bijvoorbeeld België waar deze vorm van

---

[162] *Kamerstukken II* 2000/01, 25 877, nr. 15, p. 5.

[163] In de wetsgeschiedenis is bepaald dat het gaat om gegevens 1) uit de gemeentelijke basisadministratie persoonsgegevens (artikel 88 Wet GBA), 2) door de personen en instanties als bedoeld in artikelen 61 en 62 van de Wiv 2002 (gerechtelijke instanties), en 3) uit registraties op grond van de wet justitiële documentatie en op de verklaringen omtrent het gedrag, *Kamerstukken II* 2000/01, 25 877, nr. 14, p. 37.

[164] Toezichtsrapport van de CTIVD nr. 8b inzake de inzet door de AIVD van informanten en agenten, meer in het bijzonder in het buitenland, geen kamerstuk, paragraaf 5.3, beschikbaar op www.ctivd.nl.

[165] *Kamerstukken II* 1999/2000, 25 877, nr. 8, p. 59.

[166] Toezichtsrapport van de CTIVD nr. 20 inzake de financieel-economische onderzoeken van de AIVD, *Kamerstukken II* 2008/09, 29 924, nr. 35 (bijlage), paragraaf 3.3.1, ook beschikbaar op www.ctivd.nl.

gegevensverzameling in de categorie uitzonderlijke (zeer ingrijpende) methode valt.[167] In de wetsgeschiedenis is bepaald dat artikel 17 Wiv 2002 in uitzonderlijke gevallen kan worden ingezet om op basis van vrijwilligheid zogenaamde printergegevens (dat wil zeggen gegevens achteraf uit de persoonsregistratie) van (historische) telefonieverkeersgegevens op te vragen, naast de bijzondere bevoegdheid hiertoe op grond van artikel 28 Wiv 2002 (dan geldt er overigens een medewerkingsplicht).[168]

Bij de inzet van de algemene bevoegdheid uit artikel 17 Wiv 2002 gelden enkele waarborgen. Niet alleen de eigen taakstelling stelt grenzen aan wat de diensten ingevolge artikel 17 Wiv 2002 mogen vragen aan anderen, ook de in paragraaf IV uiteengezette regels ten aanzien van de verwerking van gegevens stellen hieraan beperkingen. Van belang zijn met name de eerder besproken artikelen 12 en 13 Wiv 2002, waarin eisen worden gesteld aan de kwaliteit van de gegevensverwerking (het mag slechts plaatsvinden voor een bepaald doel en voor zover dat noodzakelijk is voor een goede uitvoering van de wet en indien het in overeenstemming met de wet en op een behoorlijke en zorgvuldige wijze geschiedt) en waarin de personen ten aanzien van wie gegevensverwerking mag plaatsvinden limitatief worden opgesomd.

V.2 Bijzondere bevoegdheden

De diensten kunnen onder strikte voorwaarden ook (persoons)gegevens(verzamelingen) verzamelen door de inzet van bijzondere bevoegdheden. Het bijzondere karakter van deze bevoegdheden is onder meer daarin gelegen dat de uitoefening ervan in het geheim geschiedt. Bovendien wordt door de toepassing van deze bevoegdheden inbreuk gemaakt op bepaalde grondrechten. De diensten zijn slechts bevoegd om bijzondere bevoegdheden in te zetten ten aanzien van bepaalde taken: voor de AIVD gaat het om de a- en d-taak, voor de MIVD om de a-, c- en e-taak. De bijzondere bevoegdheden die relevant zijn voor de verzameling van telecommunicatiegegevens worden hieronder per bevoegdheid toegelicht.

V.2.1 Artikel 21 Wiv 2002

De bevoegdheid tot de inzet van agenten is neergelegd in artikel 21 Wiv 2002:

> "de inzet van natuurlijke personen (…) die onder de verantwoordelijkheid en onder instructie van een dienst zijn belast met (1) het gericht gegevens verzamelen (…) (2) het bevorderen of treffen van maatregelen (…)"

Een agent is een persoon die doelbewust door de diensten wordt ingezet om gericht gegevens te verzamelen over personen en organisaties die voor de taakvoering van een dienst van belang kunnen zijn (artikel 21 lid 1 sub a onder 1, Wiv 2002). In de memorie van toelichting bij de Wiv 2002 wordt toegelicht dat de primaire taak van een agent is om jegens een bepaalde persoon of in een bepaalde organisatie die in het kader van een onderzoek van een dient de aandacht heeft, een zogeheten informatiepositie te verwerven en – eenmaal verworven – die ook de behouden.[169]

---

[167] H.T. Bos-Ollermann, 'Meerdere wegen naar Straatsburg. Geheime methoden en toezicht op de inlichtingen- en veiligheidsdiensten in België en Nederland', in *De orde van de dag*, afl. 56 (dec. 2011), p. 101.

[168] *Kamerstukken II* 1997/98, 25 877, nr. 3, p. 47.

[169] *Kamerstukken II* 1997/98, 25 877, nr. 3, p. 31.

Een belangrijk element van de inzet van een agent is dat de diensten de betrokken persoon *instrueren* om iets te doen. De agent werkt onder aansturing en onder supervisie van de betrokken dienst. Hierin onderscheidt de agent zich van de in artikel 17 Wiv 2002 beschreven informant.[170]

Voor de gerichtheid van de aansturing is het van belang dat de dienst goed weet wat de dienst wil bereiken met de inzet van de agent. De inzet van een agent is een heel ander soort bijzondere bevoegdheid dan bijvoorbeeld de inzet van een telefoontap. Waar bij dit laatste middel op voorhand vaststaat wat het risico van de inzet is en kan worden ingeschat hoe groot de inbreuk op de persoonlijke levenssfeer zal zijn, is dit bij de inzet van een agent minder evident. Een agent kan immers tot talloze verschillende activiteiten worden aangezet. De contacten met een onderzoekssubject kunnen oppervlakkig zijn of heel persoonlijk, de agent kan enkel zijn oor te luisteren leggen of hij kan actief participeren in activiteiten, hij kan incidenteel voor de dienst op pad worden gestuurd of dagelijks opdrachten uitvoeren. Het is niet een kwestie van een knop aan- of uitzetten, zoals bij een telefoontap. Bij iedere keuze om een agent op een bepaalde manier aan te sturen, wordt de dienst geacht een afweging te maken van de noodzakelijkheid, proportionaliteit en subsidiariteit van deze keuze (zie paragraaf III).

De toestemming voor de inzet van een agent wordt ingevolge artikel 19, derde lid, Wiv 2002 verleend voor een periode van ten hoogste drie maanden en kan telkens op een daartoe strekkend verzoek worden verlengd voor eenzelfde periode. Op grond van de Wiv 2002 wordt voor de inzet van een agent geen toestemming van de betrokken minister, dan wel het hoofd van de dienst, als voorwaarde gesteld. Bij de AIVD is voor de aanvankelijke inzet van een agent in beginsel toestemming van de betrokken directeur van de eenheid of het unithoofd nodig.[171] Voor de verlenging van de inzet is toestemming van het teamhoofd nodig. Bij de MIVD is bepaald dat de eerste toestemming door de minister dient plaats te vinden nu mandatering aan het hoofd van de dienst is uitgesloten.[172] Een verlenging van de inzet is wel aan het hoofd van de dienst gemandateerd tenzij sprake is van een principieel beleidsmatig of politiek gevoelig karakter.[173] Lagere mandatering van deze bevoegdheid is niet toegestaan binnen de MIVD.[174]

De agent kan een eigen medewerker van de dienst zijn maar ook een extern persoon, die specifiek voor deze taak wordt gezocht.[175] De agent werkt op vrijwillige basis samen met de dienst,[176] waarbij de dienst de mogelijkheid heeft hem hiervoor te belonen. Om een agent effectief en veilig in te kunnen zetten, dient de relatie tussen de AIVD of de MIVD en de agent niet bekend te zijn in de buitenwereld. Op grond van de verplichtingen in artikel 15 Wiv 2002 dienen de diensten ervoor te zorgen dat informatie over en afkomstig van een

---

[170] Toezichtsrapport van de CTIVD nr. 8b inzake de inzet door de AIVD van informanten en agenten, meer in het bijzonder in het buitenland, geen kamerstuk, paragraaf 5.3, beschikbaar op www.ctivd.nl.
[171] De mandatering van de bevoegdheid om toestemming te geven voor de inzet en de verlenging van de inzet is ter uitwerking van artikel 19 Wiv 2002 vastgelegd in het Mandaatbesluit bijzondere bevoegdheden AIVD 2009. De artikelen 4 en 5 van het Mandaatbesluit zien op het vereiste niveau van toestemming voor de inzet van agenten. Uit het Mandaatbesluit blijkt overigens dat wanneer de agent een persoon betreft met een bepaalde maatschappelijke functie, het toestemmingsniveau hoger ligt. Dit kan het niveau van directeur, hoofd van de dienst of minister zijn.
[172] Mandaatregeling Defensie Wiv 2002 en Wvo, artikel 3, vierde lid, onder a 1^0, *Stcrt.* 2002, 147.
[173] *Idem*, onder a 2^0.
[174] Ondermandaat- en machtingsbesluit MIVD 2009, artikel 3, tweede lid, *Stcrt.* nr. 7168.
[175] *Kamerstukken II* 1997/98, 25 877, nr. 3, p. 31.
[176] *Kamerstukken II* 1999/2000, 25 877, nr. 8, p. 59.

agent slechts onder strikte voorwaarden wordt verspreid en openbaar gemaakt. Uitgangspunt van de wet is de geheimhouding van daarvoor in aanmerking komende gegevens en bronnen waaruit gegevens afkomstig zijn.

V.2.2 Artikel 24 Wiv 2002

In artikel 24, eerste lid, Wiv 2002 is de bevoegdheid tot het hacken van een geautomatiseerd werk geregeld:

> "De diensten zijn bevoegd tot het al dan niet met gebruikmaking van technische hulpmiddelen, valse signalen, valse sleutels of valse hoedanigheid, binnendringen in een geautomatiseerd werk. Tot de bevoegdheid, bedoeld in de eerste volzin, behoort tevens de bevoegdheid:
>
> a. tot het doorbreken van enige beveiliging;
> b. tot het aanbrengen van technische voorzieningen teneinde versleuteling van gegevens opgeslagen of verwerkt in het geautomatiseerde werk ongedaan te maken;
> c. de gegevens opgeslagen of verwerkt in het geautomatiseerde werk over te nemen."

Voor de omschrijving van de bevoegdheid tot hacken heeft de wetgever nauw aansluiting gezocht bij de in artikel 138ab van het Wetboek van Strafrecht (Sr) gehanteerde formulering inzake de strafbaarstelling van computervredebreuk.[177] Onder "geautomatiseerd werk" moet, in navolging van artikel 80sexies Sr, worden verstaan "een inrichting die bestemd is om langs elektronische weg gegevens op te slaan, te verwerken en over te dragen". De definitie spreekt van opslag *en* verwerking *en* overdracht van gegevens. Het gaat hier dan ook om cumulatieve voorwaarden: een inrichting die enkel bestemd is om gegevens over te dragen (een eenvoudig telefoontoestel, bepaalde zend- en ontvanginrichtingen) of op te slaan (een usb-stick) valt buiten de begripsomschrijving.[178] In de wetsgeschiedenis werd aangegeven dat het in de praktijk in het bijzonder gaat om het binnendringen in (*stand-alone*) computers[179] en computernetwerken[180].

Uit het eerste lid, sub c, van artikel 24 Wiv 2002 blijkt dat onder de bevoegdheid tot binnendringen tevens de bevoegdheid behoort de gegevens opgeslagen of verwerkt in het geautomatiseerde werk over te nemen. Ook de term *overnemen* wordt uitgelegd overeenkomstig het Wetboek van Strafrecht. Volgens de wetsgeschiedenis bij artikel 138ab Sr wordt met overnemen het eigenlijke kopiëren beschreven.[181] Hoewel het logisch lijkt dat er onder overnemen in de zin van artikel 24 Wiv 2002 ook kennisnemen van de inhoud valt, blijkt dit niet als zodanig uit de wet(sgeschiedenis). Wel kan gesteld worden dat er met het overnemen van gegevens sprake is van gegevensverwerking in de zin van de Wiv 2002 (artikel 1 sub f). Omdat het overnemen van gegevens valt onder de bevoegdheid van artikel 24 Wiv 2002 dient te worden voldaan aan de vereisten die voor de inzet van bijzondere

---

[177] *Kamerstukken II* 1997/98, 25 877, nr. 3, p. 39: "Het gaat daarbij om het opzettelijk wederrechtelijk binnendringen in een geautomatiseerd werk voor de opslag of verwerking van gegevens, of een deel daarvan, waarbij enige beveiliging wordt doorbroken of de toegang wordt verworven door een technische ingreep, met behulp van valse signalen of een valse sleutel dan wel door het aannemen van een valse hoedanigheid."
[178] *Kamerstukken II* 1998/99, 26 671, nr. 3, p. 44.
[179] *Kamerstukken II* 1997/98, 25 877, nr. 3, p. 39.
[180] *Kamerstukken II* 1999/2000, 25 877, nr. 8, p. 63.
[181] *Kamerstukken II,* 1998/99, 26 671, nr. 3, p. 28

bevoegdheden gelden, namelijk dat de noodzakelijkheid, proportionaliteit en subsidiariteit van de inzet worden gemotiveerd (zie paragraaf III).

De memorie van toelichting bij artikel 24 Wiv 2002 schrijft voor dat de uitoefening van de bevoegdheid tot hacken slechts geoorloofd is indien daarvoor door de betrokken minister dan wel door het hoofd van de dienst toestemming is verleend (artikel 19 lid 1 Wiv 2002).[182] Daar waar voor een aantal gevallen bepaald is dat uitsluitend de minister toestemming kan verlenen (bijv. tappen op grond van artikel 25 Wiv 2002), wordt artikel 24 Wiv 2002 in dit kader niet genoemd door de wetgever.[183] Submandaat op grond van artikel 19, tweede lid, Wiv 2002 is daarom wettelijk toegestaan. Op grond van dit artikel kan het hoofd van de dienst aan hem ondergeschikte ambtenaren bij schriftelijk besluit aanwijzen die toestemming namens hem verlenen, wat voor artikel 24 Wiv 2002 is gebeurd in artikel 7 van het Mandaatbesluit bijzondere bevoegdheden AIVD 2009. In de Mandaatregeling van de MIVD is bepaald dat het hoofd van de dienst geen mandaat heeft ten aanzien van het eerste verzoek tot toestemming, dan wel de verlenging voor zover sprake is van een principieel beleidsmatig of politiek gevoelig karakter.[184] In die gevallen dient toestemming aan de minister van Defensie te worden gevraagd. De Commissie-Dessens heeft aanbevolen om het toestemmingsniveau voor de inzet van artikel 24 Wiv 2002 bij de betrokken minister neer te leggen. Dit vloeit voort uit de gedachtelijn van de Commissie-Dessens dat naarmate de inbreuk op de persoonlijke levenssfeer en het communicatiegeheim indringender is de toestemmingsprocedure sterker ingebed moet zijn en dat terughoudendheid betracht dient te worden met het (door)mandateren van bevoegdheden die inbreuk op grondrechten maken.[185]

Artikel 24 Wiv 2002 geeft de diensten de bevoegdheid om, bij het binnendringen in een geautomatiseerd werk, "de gegevens opgeslagen of verwerkt in het geautomatiseerde werk over te nemen". Het is dus van belang dat de gegevens zijn opgeslagen of verwerkt. Gegevens waar het om zou kunnen gaan zijn bestanden opgeslagen op een computer of server (foto's, tekstbestanden, etc.), maar ook vormen van een gesprek (een chatgesprek), telecommunicatie (een e-mail), websites of overgedragen gegevens zoals opgesomd in artikel 25 Wiv 2002. Het verschil met artikel 25 Wiv 2002 is dat bij artikel 24 Wiv 2002 de gegevens in principe *achteraf* worden overgenomen, en niet (*real time*) getapt, ontvangen, opgenomen of afgeluisterd worden. Een voorbeeld ter illustratie: bij een internettap (artikel 25 Wiv 2002) wordt een e-mail bericht onderschept tussen verzender en ontvanger, terwijl bij een artikel 24 last datzelfde e-mailbericht overgenomen wordt terwijl het bericht zich nog (of al) bij één van beide partijen bevindt. De inhoud van de informatie die via het binnendringen in een geautomatiseerd werk wordt binnengehaald kan evenwel vergelijkbaar zijn met de informatie die via een tap wordt verworven. Sterker nog, een artikel 24 last kan vaak meer opleveren. Zo kunnen met een tap op een IP-adres (artikel 25 Wiv 2002) alleen de e-mailberichten binnengehaald worden die vanaf dat specifieke IP-adres worden verstuurd en ontvangen. Met het hacken van een e-mailaccount kunnen alle e-mailberichten opgeslagen in de mailbox binnengehaald worden, onafhankelijk vanaf welke computer de berichten verstuurd zijn of op welke computer zij ontvangen zijn. Wel is het zo dat met een IP-tap (artikel 25 Wiv 2002) het berichtenverkeer van verschillende e-mailadressen binnengehaald

[182] *Kamerstukken II* 1997/98, 25 877, nr. 3, p. 39.
[183] *Kamerstukken II* 1999/2000, 25 877, nr. 8, p. 48.
[184] Mandaatregeling Defensie Wiv 2002 en Wvo, artikel 3 lid 4 onder a 1^0 en 2^0, *Stcrt.* 2002, 147.
[185] Rapport Commissie-Dessens, *Evaluatie Wet op de inlichtingen- en veiligheidsdiensten 2002. Naar een nieuwe balans tussen bevoegdheden en waarborgen*, december 2013, *Kamerstukken II* 2013/14, 33 820, nr. 1 (bijlage), p. 172.

kan worden, die vanaf één IP-adres gebruikt worden. Een artikel 24 last haalt alleen binnen wat er vanaf een specifiek e-mailadres, waarvoor de last is aangevraagd, verstuurd en ontvangen is.

Het huidige artikel 13 van de Grondwet biedt thans alleen nog bescherming aan communicatie tijdens de transportfase, zodat het binnendringen in een geautomatiseerd systeem op grond van artikel 24 hier in beginsel buiten valt. In het wetsvoorstel tot wijziging van artikel 13 wordt de bescherming van communicatie uitgebreid met de tussentijdse opslag ervan bij een derde, bijvoorbeeld berichten in een mailbox van een e-mailprovider. Artikel 13 Grondwet wordt besproken in paragraaf II.3. Het is dus voorstelbaar dat op termijn de opbrengst van de inzet van artikel 24 Wiv 2002 ook onder het telecommunicatiegeheim van artikel 13 Grondwet valt.

In het derde lid van artikel 24 Wiv 2002 is de medewerkingsplicht neergelegd, dat wil zeggen, de verplichting om mee te werken aan het ongedaan maken van de versleuteling van informatie. Ingevolge artikel 89 Wiv 2002 is het weigeren om mee te werken strafbaar gesteld.

V.2.3 Artikel 25 Wiv 2002

Artikel 25, eerste lid, Wiv 2002 bevat de bevoegdheid tot het gericht aftappen van (tele)communicatie:

> "De diensten zijn bevoegd tot het met een technisch hulpmiddel gericht aftappen, ontvangen, opnemen en afluisteren van elke vorm van gesprek, telecommunicatie of gegevensoverdracht door middel van een geautomatiseerd werk, ongeacht waar een en ander plaatsvindt. Tot de bevoegdheid, bedoeld in de eerste volzin, behoort tevens de bevoegdheid om versleuteling van de gesprekken, telecommunicatie of gegevensoverdracht ongedaan te maken."

Het artikel is algemeen en ruim geformuleerd. Het gaat om *elke vorm van* gesprek, telecommunicatie of gegevensoverdracht via een geautomatiseerd werk. Hieronder kan ook elektronische communicatie worden begrepen. Dit betekent onder andere dat niet alleen telefoon*gesprekken* kunnen worden afgetapt, maar dat ook berichtenverkeer dat plaatsvindt via een telefoonverbinding kan worden afgetapt.[186] Gedacht kan worden aan fax- of sms-berichten. Het voordeel van deze ruime formulering is dat de diensten kunnen inspelen op nieuwe communicatietechnologieën.

Op basis van artikel 25 wordt de gerichte interceptie van zowel kabelgebonden als niet-kabelgebonden communicatie door de diensten toegestaan. De diensten kunnen bijvoorbeeld gesprekken opnemen met behulp van een microfoon, telefoongesprekken aftappen, e-mailberichten lezen, het internetgedrag van een persoon in de gaten houden en *High Frequency* (HF-)radioverkeer intercepteren. Het woord "*gericht*" houdt in dat de dienst gericht kennis neemt van de inhoud van communicatie ten aanzien van een bij de dienst bekende persoon, organisatie, frequentie, telefoonnummer of IP-adres.

Tijdens de totstandkoming van de Wiv 2002 is de vraag gesteld of de woorden "ongeacht waar een en ander plaatsvindt" betekenen dat vanuit Nederland ook gesprekken, telecommunicatie en gegevensoverdracht in andere landen kunnen worden afgetapt. De regering gaf daarop het volgende antwoord:

---

[186] *Kamerstukken II* 1997/98, 25 877, nr. 3, p. 41.

> "Allereerst wordt opgemerkt dat de bevoegdheid van de diensten om gesprekken, telecommunicatie en gegevensoverdracht af te tappen, zoals onder andere geregeld in artikel 25, niet verder reikt dan tot waar de rechtsmacht van de Nederlandse Staat reikt. De Nederlandse wetgever kan immers niet eenzijdig rechtsmacht scheppen in andere landen. Dat neemt niet weg dat de uitoefening van de in artikel 25 geregelde bevoegdheid, in het bijzonder voor zover deze betrekking heeft op de interceptie van telecommunicatie, alsmede de uitoefening van de bevoegdheden, zoals neergelegd in het bij nota van wijziging ingevoegde artikel 25a [Commissie: thans artikel 26] en artikel 26 [Commissie: thans artikel 27], [zich] tevens uit kunnen strekken tot de interceptie van telecommunicatie met een oorsprong of bestemming in het buitenland."[187]

Met de inzet van de middelen genoemd in artikel 25 Wiv 2002 wordt een inbreuk gemaakt op de persoonlijke levenssfeer van betrokkenen, omdat gericht kennis wordt genomen van de inhoud van de communicatie van personen en organisaties.[188] Door de inzet van deze bijzondere bevoegdheid wordt een inbreuk gemaakt op het in artikel 13 van de Grondwet neergelegde telefoon- en telegraafgeheim. Bij de totstandkoming van de Wiv 2002 is ervoor gekozen om niet te voorzien in een mandaatregeling bij de bijzondere bevoegdheden die inbreuk maken op meer specifiek door de Grondwet geregelde rechten, zoals het huisrecht en het telefoon- en telegraafgeheim.[189] Dit betekent dat op grond van artikel 19 jo. artikel 25, tweede lid, Wiv 2002 uitsluitend de minister van BZK respectievelijk de minister van Defensie bevoegd is om aan de AIVD respectievelijk de MIVD toestemming te geven om af te tappen.[190]

Het verzoek om toestemming door (het hoofd van) een dienst aan de verantwoordelijke minister moet volgens artikel 25, vierde lid, Wiv 2002 in ieder geval bevatten:

a) een aanduiding van de bevoegdheid en, voor zover van toepassing, het nummer;
b) gegevens betreffende de identiteit van de persoon of organisatie waarop de bevoegdheid wordt ingezet;
c) de redenen van het verzoek.

In het geval er geen sprake is van gerichte interceptie van HF-radioverkeer aan de hand van een onder a bedoeld nummer maar van interceptie aan de hand van een technisch kenmerk (dat wil zeggen frequenties), hoeft, volgens de wetsgeschiedenis, dit technisch kenmerk niet vermeld te worden. Als reden hiervoor wordt gegeven dat personen en organisaties veelal via meerdere en wisselende frequenties communiceren. Het stellen van het vereiste van vermelding van het technisch kenmerk zou in de praktijk ertoe leiden dat zeer regelmatig een (hernieuwd of aanvullend) verzoek om toestemming zou moeten worden ingediend. Dit levert een onwenselijke en onwerkbare situatie op.[191]

De toestemming wordt verleend voor een periode van ten hoogste drie maanden en kan telkens worden verlengd. Dat impliceert volgens de wetgever dat, indien het noodzakelijk, proportioneel en subsidiair wordt geacht de inzet van het desbetreffende middel na afloop

---

[187] *Kamerstukken II* 1999/2000, 25 877, nr. 8, p. 65.
[188] Militair berichtenverkeer vormt een uitzondering in dezen.
[189] *Kamerstukken II* 1999/2000, 25 877, nr. 8, p. 45-46; *Kamerstukken II* 2000/01, 25 877, nr. 59, p. 7-8.
[190] Indien het gaat om plaatsen die niet in gebruik zijn bij het ministerie van Defensie, dient toestemming verleend te worden in overeenstemming met de minister van BZK (artikel 25, lid 3, Wiv 2002).
[191] *Kamerstukken II* 1999/2000, 25 877, nr. 9, p. 18-19.

van deze drie maanden te continueren, opnieuw toestemming dient te worden gevraagd door het hoofd van de dienst.[192]

Het zesde lid voorziet in de gevallen dat de gegevens over de identiteit van de persoon of organisatie waarop de bevoegdheid wordt ingezet niet bekend zijn ten tijde van het indienen van het verzoek om toestemming aan de minister. In die gevallen wordt toestemming slechts verleend onder de voorwaarde dat de desbetreffende gegevens zo spoedig mogelijk worden aangevuld.

V.2.4 Artikel 26 Wiv 2002

Artikel 26, eerste lid, Wiv 2002 voorziet in de bevoegdheid tot *searchen*:

> "De diensten zijn bevoegd tot het met een technisch hulpmiddel ontvangen en opnemen van niet-kabelgebonden telecommunicatie die zijn oorsprong of bestemming in andere landen heeft, aan de hand van een technisch kenmerk ter verkenning van de communicatie. De diensten zijn bevoegd om van daarbij ontvangen gegevens kennis te nemen. Tot de bevoegdheid, bedoeld in de eerste volzin, behoort tevens de bevoegdheid om versleuteling van telecommunicatie ongedaan te maken."

De uitoefening van de bevoegdheid tot gerichte interceptie (voor zover deze betrekking heeft op niet-kabelgebonden communicatie; artikel 25 Wiv 2002) en selectie na ongerichte interceptie (die alleen niet-kabelgebonden communicatie mag betreffen; artikel 27 Wiv 2002) hangen in de praktijk nauw samen met de bevoegdheid tot *searchen* (artikel 26 Wiv 2002).[193] Het *searchen* gaat doorgaans vooraf aan de uitoefening van deze bevoegdheden, met andere woorden het maakt de inzet van die bevoegdheden mogelijk.[194]

Bij de bevoegdheid tot *searchen* mag het uitsluitend gaan om het verkennen van niet-kabelgebonden communicatie die zijn oorsprong of bestemming in andere landen heeft; met name HF-radioverkeer en satellietcommunicatie.[195] Slechts een klein gedeelte van het HF- en satellietverkeer is van belang voor een goede taakuitoefening door de diensten. Bij het *searchen* wordt binnen het kader van de taakomschrijving door de diensten geïnventariseerd of verkend welke delen van de ether mogelijk voor interceptie in aanmerking komen.[196] Er wordt getracht te achterhalen wat de aard van de telecommunicatie is die over bepaalde frequenties of kanalen loopt (technische kenmerken, zoals wat voor zendapparatuur of transmissiesysteem) en welke persoon of organisatie de telecommunicatie verzendt (de identiteit van de afzender).[197] Bij dit laatste wordt onder meer nagegaan of het om digitale of analoge signalen gaat, welk medium (telex-, telefoon-, of dataverkeer) wordt gebruikt en in welke taal wordt uitgezonden.[198] Voorts is het *searchen* erop gericht om vast te stellen of het gaat om telecommunicatie waarvan kennisneming noodzakelijk is voor een goede taakuitvoering door de diensten.[199] Om te kunnen bepalen wie de communicatie verricht en

---

[192] *Kamerstukken II* 1997/98, 25 877, nr. 3, p. 43.
[193] Voor een uitvoerige bespreking van deze onderwerpen wordt verwezen naar het toezichtsrapport van de CTIVD nr. 28 inzake de inzet van Sigint door de MIVD, *Kamerstukken II* 2011/12, 29 924, nr. 74 (bijlage), beschikbaar op www.ctivd.nl.
[194] *Kamerstukken II* 2000/01, 25 877, nr. 14, p. 30/32.
[195] *Kamerstukken II* 1999/2000, 25 877, nr. 9, p. 23-24.
[196] *Kamerstukken II* 2000/01, 25 877, nr. 14, p. 30.
[197] *Kamerstukken II* 1999/2000, 25 877, nr. 9, p. 21.
[198] *Kamerstukken II* 2000/01, 25 877, nr. 14, p. 30.
[199] *Kamerstukken II* 1999/2000, 25 877, nr. 9, p. 21-22.

of het om een persoon of organisatie gaat die de aandacht van de diensten verdient, is het van belang om kennis te kunnen nemen van de inhoud van de telecommunicatie.[200] Dit wordt in artikel 26, eerste lid, Wiv 2002 dan ook nadrukkelijk door de wetgever toegestaan. Het kennisnemen van de inhoud geschiedt echter steekproefsgewijs, voor korte duur en vormt slechts een hulpmiddel, niet het doel van het middel.[201] Het langer volgen van een uitzending dan strikt noodzakelijk om de identiteit van de personen of organisaties vast te stellen is niet toelaatbaar. Het *searchen* zou dan immers ontaarden in een niet toegestane vorm van gericht kennisnemen van de inhoud van de communicatie.[202] Tot de bevoegdheid om te *searchen* behoort volgens het eerste lid ook de bevoegdheid om de versleuteling van de telecommunicatie ongedaan te maken.

Er kan onderscheid worden gemaakt tussen drie vormen van searchen: 1) ten behoeve van gerichte interceptie (HF-radioverkeer); 2) ten behoeve van ongerichte interceptie (satellietcommunicatie); 3) ten behoeve van selectie.

Bij searchen ten behoeve van gerichte interceptie (HF-radioverkeer) wordt steekproefsgewijs van de inhoud van berichten kennisgenomen en wordt een uitzending slechts kort gevolgd. De activiteit is niet te vergelijken met afluisteren. In de wetsgeschiedenis wordt het searchen van HF-radioverkeer vergeleken met het draaien aan een radioknop om te achterhalen welke organisatie op welke frequentie uitzendt.[203] De minister van Defensie heeft destijds uitgelegd dat er een heel wezenlijk verschil is tussen het zoeken met als doel te weten wat er op de markt beschikbaar is, zodat op het moment dat er voor een bepaald doel gerichte informatie moet worden ingewonnen, die informatie beschikbaar is, en het gericht inwinnen van informatie. Hij stelde daarbij dat wanneer er echt wordt geluisterd, de communicatie wordt opgeslagen, wordt vertaald en in een breder kader wordt geplaatst, doelgericht voor een bepaalde operatie informatie wordt verzameld. Dat valt onder het regime van toestemming (artikel 25 Wiv 2002). Alleen het bijeenbrengen van mogelijkheden valt onder het regime van "aan de knop draaien".[204]

Bij het searchen ten behoeve van ongerichte interceptie (satellietcommunicatie) is het van belang dat de diensten niet alle satellietcommunicatie die door de ether gaat kunnen ontvangen en opnemen maar daarin keuzes dienen te maken. Het searchen dient ertoe deze keuzes te optimaliseren. Door te searchen wordt bijvoorbeeld achterhaald uit welke regio de communicatie die over een bepaald satellietkanaal verloopt afkomstig is, naar welke regio de communicatie wordt verzonden en wat voor soort communicatie het betreft (spraak, fax, internet, etc.). Het searchen van satellietcommunicatie ondersteunt het proces van ongerichte interceptie (artikel 27 Wiv 2002) doordat met het searchen kan worden bekeken over welke satellietkanalen voor de taakuitvoering van de diensten mogelijk relevante communicatie verloopt.[205] Vanwege het searchen kan het satellietverkeer dat wordt ontvangen en opgenomen worden beperkt tot bepaalde kanalen.206 De diensten kunnen vervolgens een aantal satellietkanalen kiezen en de communicatie die daarover verloopt ongericht ontvangen en opnemen, om vervolgens – met toestemming van de minister – de bevoegdheid van artikel 27, derde lid, Wiv 2002 (selectie aan de hand van kenmerken) in te

[200] *Idem*, p. 21-23.
[201] *Kamerstukken II* 2000/01, 25 877, nr. 14, p. 36-37.
[202] *Idem*, p. 35.
[203] *Idem*, p. 30.
[204] *Kamerstukken II* 2000/01, 25 877, nr. 72, p. 4-6.
[205] *Kamerstukken II* 2000/01, 25 877, nr. 14, p. 32.
[206] *Kamerstukken II* 2000/01, 25 877, nr. 59, p. 12.

zetten om uit de grote hoeveelheid satellietcommunicatie die is ontvangen en opgenomen (bulk) die berichten te selecteren waarvan het kennisnemen voor de taakuitvoering van de dienst noodzakelijk is.

Bij *searchen* ten behoeve van selectie kunnen in de praktijk drie vormen worden onderscheiden: 1) het *searchen* van de bulk aan communicatie om te bepalen of met de selectiecriteria waarvoor toestemming is verkregen de gewenste communicatie kan worden gegenereerd; 2) het *searchen* van de bulk aan communicatie om potentiële onderzoekssubjecten te identificeren of te duiden; 3) het *searchen* van de bulk aan communicatie naar gegevens waaruit in het kader van een verwacht nieuw onderzoeksgebied toekomstige selectiecriteria (bijv. telefoonnummers) kunnen worden afgeleid. Het gebruik van de eerste vorm van *searchen* wordt naar het oordeel van de Commissie door de Wiv 2002 ondersteund. De andere twee vormen vinden geen ondersteuning in de Wiv 2002.[207]

In het tweede lid van artikel 26 Wiv 2002 is bepaald dat voor het *searchen* geen toestemming als bedoeld in artikel 19 Wiv 2002 is vereist. Volgens de wetsgeschiedenis bij artikel 26 Wiv 2002 is de reden hiervoor dat de aard van de activiteit voor een deel vergelijkbaar is met het ongericht ontvangen en opnemen van niet-kabelgebonden telecommunicatie op grond van artikel 27 Wiv 2002. De ongerichtheid zit hier niet zo zeer in het feit dat de diensten verschillende frequenties of satellietkanalen kunnen scannen maar dat ze op voorhand niet weten welke communicatie (aard en inhoud) daarbij van wie (persoon of organisatie) langskomt.[208] De wetgever merkt bovendien op dat een toestemmingsvereiste geen toegevoegde waarde zou hebben. Het *searchen* is niet gericht op een bepaalde persoon of organisatie. Ook is er geen specifieke reden voor het *searchen* aan te wijzen (vergelijk artikel 25, vierde lid, sub c, Wiv 2002). Dit betekent dat het toestemmingsvereiste alleen betrekking zou hebben op het algemene doel van het *searchen*, zoals in artikel 26, eerste lid, Wiv 2002 is opgenomen.[209] Dat heeft de wetgever weinig zinvol geacht.

In de wetsgeschiedenis bij de Wiv 2002 wordt gesteld dat van een inbreuk op het telefoongeheim pas sprake is, indien het kennisnemen van de inhoud van een telefoongesprek gericht is op de inhoud zelf. Indien van de inhoud van een telefoongesprek kennis wordt genomen louter als kortstondig onderdeel van een onderzoek naar de identiteit van de personen of instellingen die met elkaar communiceren, is dat geen inbreuk op het telefoongeheim. Het is volgens de wetgever veeleer vergelijkbaar met een onderzoek naar verkeersgegevens. Een dergelijk onderzoek is volgens de wetgever wel te beschouwen als een inbreuk op het recht op bescherming van de persoonlijke levenssfeer, zoals neergelegd in artikel 10 van de Grondwet, maar niet als een inbreuk op het in artikel 13 van de Grondwet neergelegde telefoon- en telegraafgeheim.[210] Door de wetgever is eveneens de vergelijking getrokken tussen het *searchen* en het inluisteren op telefoongesprekken door een aanbieder van telecommunicatienetwerken en -diensten teneinde vast te stellen of een verbinding goed verloopt. Het zou te ver gaan om het telefoongeheim zo ruim op te vatten dat ook deze technische controle en herstelwerkzaamheden, waarbij wel iets van een gesprek moet worden opgevangen, als een inbreuk daarop zouden moeten worden aangemerkt.[211]

---

[207] Toezichtsrapport van de CTIVD nr. 28 inzake de inzet van Sigint door de MIVD, *Kamerstukken II* 2011/12, 29 924, nr. 74 (bijlage), paragraaf 7.4, beschikbaar op www.ctivd.nl.
[208] *Kamerstukken II* 1999/2000, 25 877, nr. 9, p. 22.
[209] *Idem*, p. 23.
[210] *Kamerstukken II* 2000/01, 25 877, nr. 14, p. 35.
[211] *Kamerstukken II* 1999/2000, 25 877, nr. 9, p. 23.

In toezichtsrapport nr. 28 plaatst de Commissie een kritische kanttekening bij de vergelijking van *searchen* met het onderzoek naar verkeersgegevens. De wetgever gaat hiermee voorbij aan het feit dat het *searchen* wel degelijk is gericht op de inhoud van de communicatie. Er wordt immers aan de hand van de inhoud getracht de identiteit van de afzender en de relevantie van de communicatie voor de taakuitvoering van de diensten vast te stellen. Bij een onderzoek naar verkeersgegevens is dit expliciet niet het geval, daarbij wordt in het geheel geen kennis genomen van de inhoud van een bericht. Ook de vergelijking met technische controle- en herstelwerkzaamheden door een aanbieder van telecommunicatienetwerken en -diensten gaat niet op aangezien het kennisnemen van de inhoud in die gevallen een niet beoogd gevolg is van de werkzaamheden. De werkzaamheden zijn er niet op gericht.[212]

Ook het gegeven dat bij het *searchen* slechts voor een korte tijd wordt kennisgenomen van de inhoud van de communicatie en dat het niet gaat om de volledige inhoud van de communicatie doet naar het oordeel van de Commissie niets af aan het feit dat wel degelijk inbreuk wordt gemaakt op het in artikel 13 van de Grondwet neergelegde telefoon- en telegraafgeheim. Dit ongeacht de verschillende interpretaties die aan het object en de reikwijdte van het grondrecht worden gegeven. Voornoemde omstandigheden kunnen enkel een rol spelen bij het waarderen van de zwaarte van de inbreuk die wordt gemaakt. Trekt men hier de vergelijking met een postbode die een envelop opent en deze, na vluchtig gekeken te hebben naar de strekking van de ingesloten brief, weer sluit, dan is de conclusie dat het briefgeheim niet is geschonden evenmin gerechtvaardigd.[213]

De bevoegdheid te *searchen* is in de Wiv 2002 als een bijzondere bevoegdheid opgenomen. Dat betekent dat de inzet van de bevoegdheid dient te voldoen aan de vereisten van noodzakelijkheid, proportionaliteit en subsidiariteit (zie paragraaf III).

V.2.5 Artikel 27 Wiv 2002

In artikel 27, eerste lid, is de bevoegdheid tot ongerichte interceptie van niet-kabelgebonden telecommunicatie opgenomen:

> "De diensten zijn bevoegd tot het met een technisch hulpmiddel ongericht ontvangen en opnemen van niet-kabelgebonden telecommunicatie. Tot de bevoegdheid, bedoeld in de eerste volzin, behoort tevens de bevoegdheid om versleuteling van de telecommunicatie ongedaan te maken."

In tegenstelling tot artikel 25 Wiv 2002 dat voorziet in het *gericht* aftappen van de (tele)communicatie van een bij de diensten bekende persoon, organisatie of telefoonnummer, maakt artikel 27, eerste lid, Wiv 2002 het mogelijk dat de diensten ook *ongericht* telecommunicatie ontvangen en opnemen. Het gaat daarbij om niet-kabelgebonden telecommunicatie, dat wil zeggen communicatieverkeer door de lucht. In het bijzonder dient gedacht te worden aan het intercepteren van telecommunicatieverkeer dat via satellieten plaatsvindt.[214] Artikel 27 Wiv 2002 geeft niet de bevoegdheid kabelgebonden telecommunicatie ongericht te intercepteren.

---

[212] Toezichtsrapport van de CTIVD nr. 28 inzake de inzet van Sigint door de MIVD, *Kamerstukken II* 2011/12, 29 924, nr. 74 (bijlage), paragraaf 4.3.3, beschikbaar op www.ctivd.nl.
[213] *Idem.*
[214] *Kamerstukken II* 1997/98, 25 877, nr. 3, p. 44.

Gesproken wordt over *ongericht*, omdat op voorhand niet duidelijk is wat de opbrengst zal zijn en of zich daartussen voor de diensten relevante informatie bevindt. De interceptie richt zich niet op berichten die afkomstig zijn van een bepaalde persoon of organisatie of gerelateerd zijn aan een bepaald technisch kenmerk, maar haalt als het ware al het berichtenverkeer dat via een bepaald satellietkanaal wordt verzonden uit de lucht (bulk).

Bij het ongericht ontvangen en opnemen wordt nog geen kennis genomen van de inhoud van de communicatie. De bulkinformatie wordt alleen in de computersystemen opgeslagen. Met de ontvangen en opgenomen telecommunicatie kan door de diensten niets worden gedaan, behalve dat eventuele versleuteling van de gegevens ongedaan gemaakt mag worden (artikel 27 lid 1 Wiv 2002). Voor dit ongericht ontvangen en opnemen van de informatie hebben de diensten geen toestemming nodig (artikel 27 lid 2 Wiv 2002), omdat volgens de wetgever nog geen sprake is van een inbreuk op de persoonlijke levenssfeer, meer in het bijzonder het telefoon- en telegraafgeheim. De wetgever merkt bij deze bevoegdheid op weinig toegevoegde waarde te zien in het stellen van een toestemmingsvereiste. Een dergelijk toestemmingsvereiste zou slechts betrekking hebben op het satellietkanaal ten aanzien waarvan de interceptie plaatsvindt en heeft dan weinig inhoudelijke betekenis.[215]

Wil een dienst echter kennis nemen van de inhoud van de communicatie, waardoor in beginsel inbreuk wordt gemaakt op de persoonlijke levenssfeer, dan dient toestemming te worden gevraagd aan de betrokken minister (voor de AIVD is dit de minister van BZK, voor de MIVD de minister van Defensie) om de ongericht ontvangen informatie (bulk) te *selecteren*, waarna kennis kan worden genomen van dat gedeelte van de opgevangen informatie waar de selectiecriteria betrekking op hebben. De bevoegdheid om te selecteren is in artikel 27, derde lid, Wiv 2002 opgenomen:

> "De gegevens die door de uitoefening van de bevoegdheid, bedoeld in het eerste lid, zijn verzameld, kunnen door de diensten worden geselecteerd aan de hand van:
> a. gegevens betreffende de identiteit van een persoon dan wel een organisatie;
> b. een nummer als bedoeld in artikel 1.1, onder bb, van de Telecommunicatiewet, dan wel enig technisch kenmerk;
> c. aan een nader omschreven onderwerp gerelateerde trefwoorden."

Bij de onder sub a en sub b genoemde selectiecriteria gaat het bijvoorbeeld om namen of adresgegevens (sub a) dan wel om telefoonnummers of IP-adressen (sub b). De gegevensverzameling aan de hand van deze selectiecriteria heeft betrekking op concrete personen en organisaties, waardoor gesproken wordt van een *gerichte* zoekactie. Daarom dient voor het selecteren aan de hand van deze gegevens hetzelfde regime te worden gevolgd als bij de inzet van artikel 25 Wiv 2002, hetgeen betekent dat uitsluitend de betrokken minister toestemming kan geven en maximaal voor een periode van drie maanden, waarna een verzoek om verlenging voor eenzelfde periode kan worden ingediend.

Door de inzet van de bevoegdheid tot "gerichte" selectie van gegevens wordt inbreuk gemaakt op de persoonlijke levenssfeer. De zwaarte van de inbreuk is afhankelijk van de concrete omstandigheden van het geval en kan niet zonder meer gelijk worden gesteld aan de zwaarte van de inbreuk die wordt gemaakt op de persoonlijke levenssfeer door de inzet van een telefoontap. Daarbij speelt een rol dat bij selectie na ongerichte interceptie niet alle communicatie van een bepaalde persoon of organisatie wordt ontvangen en opgenomen,

[215] *Kamerstukken II* 1997/98, 25 877, nr. 3, p. 44.

maar slechts datgene wat in de bulk wordt aangetroffen en dus "bij toeval" is onderschept. Dit neemt niet weg dat selectie na ongerichte interceptie wel degelijk zeer inbreukmakend kan zijn, wanneer een dienst de communicatie van veel verschillende satellieten kan opvangen en goed in staat is die bulk aan communicatie te filteren. Het verschil met de telefoontap zit dan nog in het moment van kennisnemen van de communicatie. Bij een telefoontap is dit doorgaans *real time*, dat wil zeggen op het moment van communiceren, terwijl bij selectie na ongerichte interceptie sprake is van het achteraf kennisnemen van de inhoud van de communicatie. Ook dit onderscheid is overigens betrekkelijk aangezien het veelvuldig voorkomt dat een telefoontap pas op een later moment wordt uitgeluisterd en het bij selectie van communicatie niet altijd zeker is dat het bericht door de ontvanger is gelezen op het moment van kennisnemen door een dienst.[216]

Voor de selectie aan de hand van aan een nader omschreven onderwerp gerelateerde trefwoorden (sub c) is een afwijkende regeling getroffen. De gegevensverzameling is in dit geval niet gericht op een persoon of organisatie, maar is in algemene zin van belang voor de onderzoeken waar een dienst mee bezig is (bijvoorbeeld proliferatie van chemische wapens).[217] De trefwoorden hebben dan ook geen betrekking op personen of organisaties, maar op een bepaald onderwerp. Bij de invoering van deze bevoegdheid in de Wiv 2002 is de volgende verduidelijking gegeven:

> "Een aan een onderwerp gerelateerde trefwoordenlijst zal in de regel bestaan uit (combinaties van) specifieke technische termen en aanduidingen in diverse talen. Zo'n lijst wordt zodanig opgesteld dat het selectiesysteem optimaal wordt gebruikt om de gewenste informatie te vinden. Zo zal een te gebruiken trefwoordenlijst in het kader van een onderzoek naar proliferatie van bepaalde dual use goederen naar een bepaald land of bepaalde regio onder andere kunnen bestaan uit namen van bepaalde chemische stoffen en chemische verbindingen in combinatie met die landen of regio. Een enigszins gesimplificeerd voorbeeld betreft het zoeken naar berichten waarin of het woord natrium of sodium voorkomt en tevens binnen twee posities ook het woord chlorid of fluorid. Een te hanteren lijst van trefwoorden bij een onderzoek naar de export van een raketsysteem naar bepaalde landen of regio's zou kunnen bestaan uit diverse namen waarmee het specifieke raketsysteem wordt aangeduid, eventuele projectbenamingen of aanduidingen van de diverse elementen die deel uit maken van het betreffende systeem."[218]

Net als bij artikel 25, tweede lid, Wiv 2002, zijn de diensten pas bevoegd aan de hand van trefwoorden te bekijken of zich in de ongericht ontvangen en opgenomen niet-kabelgebonden telecommunicatie informatie bevindt die relevant is voor het onderzoek, indien de dienst daarvoor toestemming heeft gekregen van de betrokken minister (artikel 27 leden 4 en 5 Wiv 2002). Omdat de persoonlijke levenssfeer van personen en organisaties hierbij niet direct in het geding is – immers de gegevensverzameling is *niet gericht* op personen of organisaties – kan de betrokken minister voor een langere periode toestemming geven om te selecteren in het kader van een onderzoek naar een nader omschreven onderwerp, namelijk voor ten hoogste één jaar. Het toestemmingsverzoek dient ten minste een nauwkeurige omschrijving van het onderwerp en de reden van de selectie te bevatten (lid 5). Volgens de wetsgeschiedenis waarborgen deze voorwaarden dat de minister over het voor het verlenen van de toestemming benodigde inzicht beschikt. Voor dat inzicht hebben de aan de onderwerpen gerelateerde trefwoorden geen toegevoegde waarde. Een aan een onderwerp gerelateerde trefwoordenlijst zal in de regel bestaan uit (combinaties van)

---

[216] Een e-mail bericht kan bijvoorbeeld lange tijd ongelezen in de inbox blijven staan.
[217] *Kamerstukken II* 1997/98, 25 877, nr. 3, p. 45.
[218] *Kamerstukken II* 2000/01, 25 877, nr. 14, p. 33.

specifieke technische termen en aanduidingen in diverse talen. Aangezien de trefwoorden dikwijls kunnen wijzigen is voorts bepaald dat de trefwoorden kunnen worden vastgesteld door het hoofd van de dienst of namens deze een door hem aangewezen ambtenaar (lid 6). Een dergelijke lijst wordt zodanig opgesteld dat het selectiesysteem optimaal wordt gebruikt om de gewenste informatie te vinden. Bij de AIVD is ervoor gekozen deze bevoegdheid uitsluitend te laten uitoefenen door het hoofd van de AIVD. In het Ondermandaat- en machtigingsbesluit MIVD 2009 zijn het hoofd en de analisten van de afdeling Sigint van de MIVD gemachtigd om de trefwoorden vast te stellen.[219] In de wetsgeschiedenis is bepaald dat van de selectie onder c zeer selectief (voornamelijk beperkt tot satellietverkeer) en terughoudend gebruik gemaakt zal worden.[220]

Het is niet uitgesloten dat gegevens die aan de hand van de selectiecriteria uit artikel 27, derde lid, Wiv 2002 niet zijn geselecteerd, en waarvan dus ook niet van de daadwerkelijke inhoud kennis kan worden genomen, niettemin relevante informatie bevatten die aan de hand van nader vast te stellen selectiecriteria alsnog zouden kunnen worden geselecteerd. Dergelijke nader vast te stellen selectiecriteria kunnen voortkomen uit informatie die aan andere bronnen van een dienst is ontleend of is ontleend aan op een later tijdstip ontvangen en opgenomen gegevens.[221]

Een voorbeeld uit de wetsgeschiedenis. Bij het zoeken op trefwoorden (artikel 27 lid 3 onder c Wiv 2002) worden soms berichten geselecteerd, waaruit blijkt dat een schip chemicaliën of goederen vervoert die kunnen worden gebruikt voor de productie van massavernietigingswapens, zonder dat echter uit de onderschepte berichten duidelijk wordt wie leverancier of afnemer van de goederen is. Met behulp van nieuwe trefwoorden, die ontleend worden aan de in eerste instantie onderschepte berichten, kan vervolgens worden bezien of aanvullende informatie over leverancier en afnemer kan worden gevonden in al eerder geïntercepteerd, maar niet geselecteerd berichtenverkeer. Bovendien is het soms mogelijk om langs deze weg vast te stellen of de relatie tussen de leverancier en de afnemer al langer bestaat. Indien de gegevens afkomstig uit ontvangen en opgenomen telecommunicatie als bedoeld in artikel 27, eerste lid, Wiv 2002 na de eerste selectie al zouden moeten worden vernietigd, zou een nadere selectie – zoals hiervoor geschetst – met als mogelijkheid een verdere verrijking en aanvulling van voor actuele onderzoeken relevante informatie niet kunnen plaatsvinden. Dit achtte de wetgever een onwenselijke situatie. Onder voorwaarden dient een dergelijke nadere selectie, die dus een zekere bewaartermijn voor de desbetreffende gegevens met zich brengt, mogelijk te zijn.[222]

Gegevens die ongericht zijn geïntercepteerd maar niet zijn geselecteerd mogen, ingevolge artikel 27, negende lid, Wiv 2002, worden bewaard voor een periode van maximaal een jaar ten behoeve van nadere selectie. Hieraan zijn in de wet twee voorwaarden gesteld. De selectie mag slechts plaatsvinden in het kader van een onderzoek op grond van een reden als bedoeld in het vierde lid, sub b, of met betrekking tot een onderwerp als bedoeld in het vijfde lid, sub a, waarvoor op het moment van het ontvangen en opnemen van de desbetreffende gegevens toestemming was verleend (lid 9 sub a). De wetgever heeft het niet wenselijk geacht dat de hier bedoelde gegevens ook beschikbaar komen voor selectie ten behoeve van onderzoeken van een dienst, die op het moment van het ontvangen en opnemen van de telecommunicatie niet actueel waren; de interceptie vond immers indertijd

---

[219] *Staatscourant* nr. 7168, artikel 3 lid 1 sub e en sub j.
[220] *Kamerstukken II* 1997/98, 25 877, nr. 3, p. 45.
[221] *Kamerstukken II* 1999/2000, 25 877, nr. 9, p. 26-27.
[222] *Idem*.

plaats ten behoeve van op dat moment actuele onderzoeken. De selectie moet voorts voor de goede uitoefening van het desbetreffende onderzoek dringend worden gevorderd (lid 9 sub b). Volgens de wetsgeschiedenis zijn deze voorwaarden opgenomen omdat een nadere selectie op geïntercepteerde gegevens niet onbeperkt en ongeclausuleerd mogelijk is. Artikel 8 EVRM staat hieraan in de weg.[223]

Artikel 27, tiende lid, Wiv 2002 verklaart het negende lid van overeenkomstige toepassing op gegevens waarvan de versleuteling nog niet ongedaan is gemaakt, met dien verstande dat de bewaartermijn van één jaar pas aanvangt met ingang van het moment waarop de versleuteling ongedaan is gemaakt.

V.2.6 Artikel 28 Wiv 2002

In artikel 28, eerste lid, Wiv 2002 is de volgende bevoegdheid neergelegd:

> "De diensten zijn bevoegd zich te wenden tot de aanbieders van openbare telecommunicatienetwerken en openbare telecommunicatiediensten in de zin van de Telecommunicatiewet met het verzoek om gegevens te verstrekken over een gebruiker en het telecommunicatieverkeer met betrekking tot die gebruiker. Het verzoek kan slechts betrekking hebben op gegevens die bij algemene maatregel van bestuur zijn aangewezen en kan zowel gegevens betreffen die ten tijde van het verzoek zijn verwerkt als gegevens die na het tijdstip van het verzoek worden verwerkt."

Op grond van deze bepaling zijn de diensten bevoegd tot het opvragen van (telefonie)verkeersgegevens bij aanbieders van openbare telecommunicatienetwerken en openbare telecommunicatiediensten. De bevoegdheid mag enkel worden toegepast ten aanzien van een "gebruiker" dat wil zeggen een bepaalde persoon. Er kunnen via artikel 28 Wiv 2002 geen algemene of ongerichte verzoeken tot het verstrekken van (telefonie) verkeersgegevens worden gedaan. De bevoegdheid ziet alleen op de categorieën verkeersgegevens die bij algemene maatregel van bestuur limitatief zijn aangewezen.[224] Volgens het Besluit ex artikel 28 Wiv 2002 zijn verkeersgegevens gegevens over de gebruiker en het telecommunicatieverkeer met betrekking tot die gebruiker. Het begrip verkeersgegevens is in dit besluit ruimer dan het begrip in de Telecommunicatiewet, omdat het mede de gebruikersgegevens, zoals naam, adres, woonplaats, nummer en de soort diensten waarvan de gebruiker maakt of heeft gemaakt, omvat. Voor wat betreft de gebruikersgegevens wordt in de nota van toelichting bij het besluit aangegeven dat deze gegevens dienen te worden opgevraagd via het systeem en de procedures van het Centraal Informatiepunt Onderzoek Telecommunicatie (CIOT).[225] De diensten hebben hiervoor een afzonderlijke bevoegdheid in artikel 29 Wiv 2002. Onder telecommunicatie wordt volgens het Besluit niet alleen kabelgebonden telecommunicatie begrepen, maar alle vormen van telecommunicatie die via openbare netwerken of diensten worden overgedragen,

---

[223] *Idem.*

[224] Artikel 2 van het Besluit ex artikel 28 Wiv 2002: Een verzoek kan betrekking hebben op gegevens betreffende de gebruiker (naam, adres, woonplaats, nummer), betreffende de personen of organisaties met wie de gebruiker verbinding heeft (gehad) of heeft getracht tot stand te brengen ofwel die hebben getracht verbinding met de gebruiker tot stand te brengen (naam, adres, woonplaats, telefoonnummer), gegevens betreffende de verbinding zelf (starttijd, eindtijd, locatiegegevens randapparatuur, nummers randapparatuur) en gegevens betreffende het abonnement (de soort diensten waarvan de gebruiker gebruik maakt of heeft gemaakt, de gegevens van degene die de rekening betaalt).

[225] Nota van toelichting bij Besluit ex artikel 28 Wiv 2002, te raadplegen via http://wetten.overheid.nl.

uitgezonden of ontvangen, zoals mobiele telecommunicatie, telecommunicatie via de kabel en satelliet. Op grond van het besluit kunnen de diensten gegevens verkrijgen over onder meer de data en tijdstippen waarop iemand heeft gebeld, met welke telefoonnummers het contact heeft plaatsgevonden en de locatie.[226] Er kunnen gegevens worden opgevraagd betreffende uitgaand verkeer: verkeer met nummers die zijn of worden opgeroepen dan wel waarmee verbindingen zijn of worden gelegd vanaf een in het verzoek aangegeven nummer. Het kan ook gaan om inkomend verkeer: verkeer met nummers waar vanaf oproepen zijn of worden gedaan en verbindingen zijn of worden gelegd met een in het verzoek aangegeven nummer.[227]

In artikel 28, eerste lid, Wiv 2002 is bepaald dat het verzoek betrekking kan hebben op zowel gegevens die ten tijde van het verzoek zijn verwerkt als op gegevens die na het tijdstip van het verzoek worden verwerkt. De diensten kunnen de telecommunicatieaanbieders aldus vragen naar het belgedrag van een persoon over bijvoorbeeld de afgelopen maand, maar de diensten kunnen ook vragen om op de hoogte te worden gehouden van het belgedrag in bijvoorbeeld de komende twee weken. Een technische voorziening maakt het in dat laatste geval mogelijk dat de diensten direct (*real time*) de beschikking krijgt over het actuele belgedrag van een persoon. Dit wordt ook wel een "stomme tap" genoemd, omdat geen kennis wordt genomen van de inhoud van de communicatie.

Op grond van de zogenaamde Europese richtlijn dataretentie (2006)[228] werd harmonisatie beoogd van de nationale regelgeving van de lidstaten van de Europese Unie waarbij aanbieders van elektronische communicatiediensten of openbare communicatienetwerken verplicht zijn tot het bewaren van bepaalde telecommunicatiegegevens (verkeers- en locatiegegevens en gebruikersgegevens) gedurende een bepaalde tijd met het oog op bestrijding van ernstige criminaliteit. In Nederland is de Richtlijn geïmplementeerd in de Wet bewaarplicht telecommunicatiegegevens (2009). Dit heeft geleid tot een bewaartermijn in de Telecommunicatiewet (artikel 13.2a): twaalf maanden voor gegevens in verband met telefonie, zes maanden voor gegevens in verband met internettoegang. Ingevolge artikel 13.4 van de Telecommunicatiewet geldt voor aanbieders van openbare telecommunicatienetwerken en -diensten de verplichting om bepaalde informatie of gegevens te verstrekken als de AIVD of de MIVD daartoe een verzoek doet op grond van artikel 28 of artikel 29 (medewerkingsplicht).[229]

Artikel 28 Wiv 2002 is niet bedoeld om kennis te nemen van de inhoud van de communicatie die via de telefoonverbinding plaatsvindt. In dat geval zou op grond van artikel 25 Wiv 2002 toestemming moeten worden gevraagd aan de betrokken minister, omdat het daarbij gaat om het ontvangen van (elke vorm van) telecommunicatie. Dit verschil is tijdens de totstandkoming van de Wiv 2002 zijdelings aan de orde gekomen op het moment dat werd gesproken over het monitoren van militair berichtenverkeer:

> "Wij menen dat van een inbreuk op het telefoongeheim sprake is, indien het kennis nemen van de inhoud van een telefoongesprek gericht is op de inhoud zelf. Indien van de inhoud van

[226] Voor een volledige opsomming van de gegevens die kunnen worden opgevraagd, zie artikel 2 van Besluit ex artikel 28 Wiv 2002.
[227] *Kamerstukken II* 1997/98, 25 877, nr. 3, p. 46.
[228] Richtlijn nr. 06/24/EG van het Europees Parlement en de Raad van 15 maart 2006 betreffende de bewaring van gegevens die zijn gegenereerd of verwerkt in verband met het aanbieden van openbaar beschikbare elektronische communicatiediensten of van openbare communicatienetwerken en tot wijziging van Richtlijn nr. 02/58/EG, inwerkingtreding 3 mei 2006, *Pb EU*, L105/54.
[229] *Kamerstukken II* 2000/01, 25 877, nr. 14, p. 37.

> een telefoongesprek kennis wordt genomen louter als kortstondig onderdeel van een onderzoek naar de identiteit van de personen of instellingen die met elkaar communiceren, zien wij dat niet als inbreuk op het telefoongeheim. Het [Commissie: monitoren van militair berichtenverkeer] is veeleer vergelijkbaar met een onderzoek naar verkeersgegevens. Een dergelijk onderzoek is wel te beschouwen als een inbreuk op het recht op privacy, zoals vastgelegd in artikel 10 van de Grondwet, doch niet als een inbreuk op het in artikel 13 van de Grondwet vastgelegde telefoongeheim."[230]

Voor het opvragen van (telefonie)verkeersgegevens is geen toestemming van de betrokken minister vereist (artikel 28 lid 3 Wiv 2002). Voldoende is dat het verzoek aan de telecommunicatieaanbieders wordt gedaan door het hoofd van de dienst (artikel 28 lid 4 Wiv 2002). De redenen om af te zien van het toestemmingsvereiste hangen samen met het geringe inbreukmakende karakter van het middel en de voorziene toepassing ervan. Uit de wetsgeschiedenis blijkt dat het middel van artikel 28 Wiv 2002 als minder ingrijpend wordt gezien dan een telefoontap, omdat dan kennis wordt genomen van de inhoud van gesprekken. Het werd voorzien dat een verzoek op grond van artikel 28 Wiv 2002 vaak vooraf zal gaan aan een verzoek om een telefoontap, omdat langs de weg van artikel 28 Wiv 2002 nadere gegevens kunnen worden verzameld die mede van belang kunnen zijn voor de vraag of en, zo ja, ten aanzien van welke persoon of organisatie een telefoontap noodzakelijk wordt geacht. In dat geval kan artikel 28 Wiv 2002 er mede toe bijdragen dat het zwaardere middel van de telefoontap slechts in die gevallen wordt ingezet waarin dat strikt noodzakelijk wordt geacht.[231]

In de memorie van toelichting bij het wetsvoorstel vorderen gegevens telecommunicatie in het kader van het Wetboek van Strafvordering is overwogen dat verkeersgegevens inzicht kunnen geven in het telecommunicatiegedrag van een gebruiker en het patroon van contacten van een persoon, waardoor een min of meer volledig beeld van bepaalde aspecten van iemands leven kan ontstaan. Hierdoor kan het opvragen van deze gegevens een inbreuk vormen op de persoonlijke levenssfeer van de betrokken persoon.[232] In dat geval is van belang dat wordt voldaan aan de eisen die het EVRM stelt zoals kwaliteitseisen aan de wettelijke regeling en voldoende wettelijke waarborgen tegen willekeur en misbruik (zie hierover paragraaf II.2). Dit geldt volgens de genoemde memorie van toelichting bij het wetsvoorstel niet voor gebruikersgegevens, dat wil zeggen gegevens die bijdragen aan het identificeren van een persoon, zoals naam, adres, woonplaats, nummer en soort telefoniedienst, aangezien dit een veel beperktere categorie gegevens betreft.[233] Hierbij doet zich wel de situatie voor dat de gegevens voor een ander doel worden gebruikt dan waartoe ze door de aanbieder zijn verwerkt. Ingevolgde het Databeschermingsverdrag van de Raad van Europa is afwijkend doelgebruik mogelijk mits dit bij wet is voorzien en met voldoende waarborgen is omkleed, noodzakelijk is met het oog op een legitiem doel en niet bovenmatig is.[234]

---

[230] *Idem*, p. 35.
[231] *Kamerstukken II* 1997/98, 25 877, nr. 3, p. 47.
[232] *Kamerstukken II* 2001/02, 28 059, nr. 3, p. 4.
[233] *Idem*, p. 5.
[234] *Idem*, p. 6.

V.2.7 Artikel 29 Wiv 2002

In artikel 29, eerste lid, Wiv 2002 is het volgende neergelegd:

> "De diensten zijn bevoegd zich te wenden tot de aanbieders van openbare telecommunicatienetwerken en openbare telecommunicatiediensten in de zin van de Telecommunicatiewet met het verzoek gegevens te verstrekken terzake van naam, adres, postcode, woonplaats, nummer en soort dienst van een gebruiker van telecommunicatie."

Deze bevoegdheid ziet op het opvragen van gebruikersgegevens of abonneegegevens (zogenaamde NAW-gegevens, nummers van de gebruiker en de soort diensten waarvan de gebruiker gebruik maakt of heeft gemaakt[235]) bij aanbieders van openbare telecommunicatienetwerken en -diensten van een natuurlijke of rechtspersoon die met de aanbieder een overeenkomst is aangegaan met betrekking tot het gebruik van een openbaar telecommunicatienetwerk of de levering van een openbare telecommunicatiedienst, alsmede een natuurlijke of rechtspersoon die hiervan daadwerkelijk gebruik maakt (lid 2). De bevoegdheid mag enkel worden toegepast ten aanzien van een "gebruiker" dat wil zeggen een bepaalde persoon. Er kunnen via artikel 29 Wiv 2002 geen algemene of ongerichte verzoeken tot het verstrekken van gebruikersgegevens worden gedaan.

Net als bij artikel 28 Wiv 2002, geldt ingevolge de Telecommunicatiewet (artikel 13.4) voor aanbieders van openbare telecommunicatienetwerken en -diensten ook bij artikel 29 Wiv 2002 de verplichting om bepaalde informatie of gegevens te verstrekken aan de AIVD en de MIVD als daar op grond van deze bijzondere bevoegdheid om wordt gevraagd.[236]

Ingevolge het vierde lid van artikel 13.4 van de Telecommunicatiewet is in het Besluit verstrekking gegevens telecommunicatie (CIOT-besluit) het Centraal Informatiepunt Onderzoek Telecommunicatie (CIOT) ingesteld en geregeld welke gebruikersgegevens aanbieders beschikbaar dienen te houden voor bevraging alsmede de wijze waarop de bevraging via het CIOT verloopt.[237] Het opvragen van gebruikersgegevens door de diensten verloopt geautomatiseerd via het CIOT.

Indien de gegevens noodzakelijk zijn om een tap (artikel 25 Wiv 2002) te kunnen aanvragen, dient de informatie opgevraagd te worden op grond van het zevende lid van die bepaling. Volgens de wetsgeschiedenis kan artikel 29 Wiv 2002 de diensten ook in staat stellen nader onderzoek te doen indien zij de beschikking krijgen over een telefoonnummer dat mogelijk wordt gebruikt door iemand die bijvoorbeeld betrokken is bij terroristische activiteiten en dit nummer naar de verblijfplaats van de persoon kan leiden.[238]

Hoewel de bevoegdheid op grond van artikel 29 Wiv 2002 niet als heel ingrijpend (inbreukmakend) wordt gezien, betreft het wel een bijzondere bevoegdheid – ook al blijkt uit de wetsgeschiedenis niet expliciet de reden hiervoor – die daarom, net als de bevoegdheid uit artikel 28 Wiv 2002, gericht dient te worden ingezet en dient te worden voorzien van een

---

[235] Uit artikel 2, onder g, volgt dat onder "diensten" zowel de telecommunicatiediensten in de zin van de Telecommunicatiewet, waarbij sprake is van het overbrengen van signalen via telecommunicatienetwerken, als de daaraan gerelateerde voorzieningen zoals een doorschakelfunctie of een geautomatiseerde telefoonbeantwoorder worden begrepen; nota van toelichting bij Besluit ex artikel 28 Wiv 2002, te raadplegen via http://wetten.overheid.nl.

[236] *Kamerstukken II* 2000/01, 25 877, nr. 14, p. 37.

[237] Besluit van 26 januari 2000, *Stb.* 2000, 71.

[238] *Kamerstukken II* 1997/98, 25 877, nr. 3, p. 48.

(interne) motivering over de noodzakelijkheid, proportionaliteit en subsidiariteit van de inzet, ook al wordt een schriftelijke motivering niet door de wet vereist.[239]

VI Samenwerking met buitenlandse inlichtingen- en/of veiligheidsdiensten

VI.1 Artikel 59: zorgplicht voor het onderhouden van relaties

Artikel 59, eerste lid, Wiv 2002 legt aan de hoofden van de AIVD en de MIVD een zorgplicht op om relaties (verbindingen) te onderhouden met daarvoor in aanmerking komende inlichtingen- en/of veiligheidsdiensten van andere landen.[240] In de wetsgeschiedenis wordt onderkend dat het met het oog op het effectief en efficiënt functioneren van de diensten onontbeerlijk is dat samenwerking met inlichtingen- en veiligheidsdiensten van andere landen plaatsvindt, juist ook vanwege het grensoverschrijdende en internationale karakter van veiligheidsproblemen.[241] Voor een adequate taakuitvoering door de diensten is het noodzakelijk dat de diensten waar mogelijk samenwerken met buitenlandse diensten.[242]

De samenwerking van de AIVD en de MIVD met buitenlandse diensten wordt in beginsel genormeerd door de algemeen geldende bepalingen in de Wiv 2002 omtrent gegevensverwerking. De leden 2 t/m 6 van artikel 59 Wiv 2002 voorzien in een aantal mogelijkheden om samen te werken met andere diensten indien de AIVD of de MIVD hierbij geen direct belang heeft. Dit vormt dus een uitzondering op de hoofdregel dat de samenwerking met andere diensten in beginsel plaatsvindt in het kader van de eigen taakuitvoering van de AIVD en de MIVD.

In de wetsgeschiedenis wordt vermeld dat afgesproken is dat de AIVD contacten onderhoudt met civiele inlichtingen- en/of veiligheidsdiensten en de MIVD met militaire inlichtingen- en/of veiligheidsdiensten en met verbindingsinlichtingendiensten. Wanneer de uitvoering van de taken van de diensten dat vergt, lichten de hoofden van de AIVD en de MIVD elkaar in wanneer contact moet worden opgenomen met militaire respectievelijk civiele diensten.[243]

Samenwerking met buitenlandse inlichtingen- en veiligheidsdiensten is van belang voor de nationale veiligheid. Hierbij dient echter niet uit het oog te worden verloren dat deze samenwerking, en dan met name de uitwisseling van gegevens, een inmenging in de grondrechten van burgers kan inhouden. In het geval van uitwisseling van persoonsgegevens zal daarvan per definitie sprake zijn. Dat kan vergaande consequenties inhouden voor de persoonlijke levenssfeer van individuen. De wetgever heeft dit spanningsveld onderkend. Zoals in de gehele Wiv 2002, is er ook bij de invulling van de regels en procedures over samenwerking tussen diensten gezocht naar een balans tussen het belang van de nationale veiligheid dat gediend wordt door samenwerking met buitenlandse diensten en het belang van de grondrechten van burgers dat hierdoor en dan met name door

---

[239] Toezichtsrapport van de CTIVD nr. 25 inzake het handelen van de MIVD jegens twee geschorste medewerkers, *Kamerstukken* II 2009/10, 29 924, nr. 59 (bijlage), paragraaf 4.2, beschikbaar op www.ctivd.nl.

[240] Zie voor een uitvoerige bespreking van dit onderwerp het toezichtsrapport van de CTIVD nr. 22a inzake de samenwerking van de AIVD met buitenlandse inlichtingen- en/of veiligheidsdiensten, *Kamerstukken II* 2009/10, 29 924, nr. 39 (bijlage), beschikbaar op www.ctivd.nl.

[241] *Kamerstukken II* 1997/98, 25 877, nr. 3, p. 73.

[242] *Kamerstukken II* 1999/2000, 25 877, nr. 8, p. 101.

[243] *Kamerstukken II* 1997/98, 25 877, nr. 3, p. 73.

uitwisseling van (persoons)gegevens onder druk komt te staan. In de wet en de wetsgeschiedenis zijn enkele belangrijke waarborgen neergelegd die de persoonlijke levenssfeer van burgers beogen te beschermen. Deze worden hieronder toegelicht.

De AIVD en de MIVD mogen niet zomaar met iedere buitenlandse dienst een samenwerkingsrelatie aangaan. In de wetsgeschiedenis is bepaald dat een aantal zaken dient te worden onderzocht voordat de AIVD dan wel de MIVD een samenwerkingsrelatie met een inlichtingen- en/of veiligheidsdienst van een ander land mag aangaan. Hierbij dient te worden bezien hoe het gesteld is met de democratische inbedding van de dienst en respect voor mensenrechten, de professionaliteit en betrouwbaarheid, het karakter van de dienst, of internationale verplichtingen samenwerking wenselijk maken en in hoeverre de samenwerking met een dienst de nationale veiligheid kan bevorderen.[244] Aan de hand van deze criteria dienen de AIVD en de MIVD te toetsen of een buitenlandse dienst in aanmerking komt voor samenwerking en welke vormen van samenwerking in beginsel toelaatbaar zijn. Deze beoordeling wordt in beginsel op het niveau van de dienst zelf gemaakt. De betrokken minister wordt hierover geïnformeerd. Indien de samenwerking een dienst van een zogenaamd "risicoland" betreft, dan dient de minister in de besluitvorming hierover te worden betrokken.[245]

De activiteiten van de AIVD en de MIVD die in het kader van de samenwerking met buitenlandse diensten plaatsvinden worden genormeerd door de bepalingen in de Wiv 2002 omtrent gegevensverwerking. Voor zover samenwerking plaatsvindt ten behoeve van de belangen van de buitenlandse dienst is artikel 59, tweede t/m zesde lid, Wiv 2002 van toepassing. Ten aanzien van de specifieke vormen van samenwerking die in artikel 59 Wiv 2002 worden genoemd (namelijk: het verstrekken van gegevens en het bieden van technische ondersteuning aan een buitenlandse dienst), bepaalt dit artikel dat deze alleen mogen plaatsvinden als de door de buitenlandse dienst te behartigen belangen niet onverenigbaar zijn met de belangen die de Nederlandse dienst heeft te behartigen en als een goede taakuitvoering door de Nederlandse dienst zich niet tegen samenwerking verzet. Volgens de wetsgeschiedenis geschiedt de beoordeling of wellicht sprake is van tegenstrijdige belangen mede aan de hand van het Nederlandse buitenlandse beleid, waaronder dat op het gebied van de mensenrechten.[246] Soms zijn de belangen die de dienst heeft te behartigen vertaald in concreet vastgesteld regeringsbeleid, zoals het mensenrechtenbeleid, maar vaak ook niet. Het gaat om een veelheid aan belangen.[247] Een aanknopingspunt in de taakomschrijving van de diensten werd niet noodzakelijk geacht. In de wet is gesteld dat de AIVD en de MIVD hun taken verrichten in ondergeschiktheid aan de wet (artikel 2 Wiv 2002). Dit houdt in dat de normen, en zeker ook de grond- en mensenrechten, die zijn neergelegd in de Grondwet en in de internationale verdragen (onder andere het EVRM) die door Nederland zijn geratificeerd, eveneens tot de belangen die de diensten hebben te behartigen moeten worden gerekend.[248] Voor wat betreft de vraag wanneer een goede taakuitvoering van een dienst zich tegen verstrekking van gegevens of technische ondersteuning aan een buitenlandse dienst verzet, is dit bijvoorbeeld aan de orde indien daardoor eigen lopende operaties van de AIVD of

[244] *Kamerstukken II* 2000/01, 25 877, nr. 59, p. 16. Zie ook het toezichtsrapport van de CTIVD nr. 22a inzake de samenwerking van de AIVD met buitenlandse inlichtingen- en/of veiligheidsdiensten, *Kamerstukken II* 2009/10, 29 924, nr. 39 (bijlage), paragraaf 5, beschikbaar op www.ctivd.nl.
[245] *Kamerstukken II* 1999/2000, 25 877, nr. 8, p. 102 en *Aanhangsel Handelingen II* 2004/05, nr. 749.
[246] *Kamerstukken II* 1997/98, 25 877, nr. 3, p. 74.
[247] *Kamerstukken II* 1999/2000, 25 877, nr. 8, p. 101.
[248] *Kamerstukken II* 2000/01, 25 877, nr. 14, p. 65.

MIVD worden gefrustreerd. In dit kader dient ook te worden beoordeeld of het verzoek past binnen de juridische kaders die de diensten in acht hebben te nemen.[249]

De praktijk van de samenwerking tussen diensten brengt bepaalde beperkingen met zich mee op het gebied van openheid over de herkomst van gedeelde gegevens. Dit is ook onderkend in de wetsgeschiedenis. Daar wordt overwogen dat het in het verkeer tussen diensten niet gebruikelijk is om actief te informeren naar dan wel de ander te informeren over de methoden die gehanteerd zijn om bepaalde informatie boven water te krijgen. Net als de AIVD en de MIVD hechten buitenlandse diensten eraan om bronnen en modus operandi geheim te houden.[250] Ten aanzien van menselijke bronnen is dit meestal een wettelijke plicht, net zoals dit voor de AIVD en de MIVD het geval is (artikel 15 Wiv 2002). Al naar gelang de aard van de samenwerkingsrelatie die bestaat met een buitenlandse dienst kan er op dit punt over en weer wel meer openheid worden gegeven, met name in de gevallen dat gezamenlijke operaties worden uitgevoerd.[251]

VI.2 Verstrekken van gegevens

VI.2.1 Wettelijke grondslag

De Wiv 2002 kent een gesloten verstrekkingsregime, wat betekent dat externe verstrekking van gegevens, dat wil zeggen aan andere personen of instanties, slechts kan plaatsvinden indien hiervoor een specifieke wettelijke basis bestaat.

De Wiv 2002 voorziet in twee wettelijke grondslagen voor gegevensverstrekking aan buitenlandse diensten. Voor verstrekking van gegevens in het kader van de eigen taak van de Nederlandse diensten vormt artikel 36, eerste lid, sub d, Wiv 2002 de wettelijke basis. Hierin is bepaald dat de diensten in het kader van een goede taakuitvoering bevoegd zijn om over door of ten behoeve van de dienst verwerkte gegevens mededeling te doen aan daarvoor in aanmerking komende inlichtingen- en veiligheidsdiensten van andere landen, alsmede andere daarvoor in aanmerking komende internationale beveiligings-, verbindingsinlichtingen- en inlichtingenorganen.

Indien het belang van de buitenlandse dienst leidend is, vormt artikel 59, tweede lid, Wiv 2002 de wettelijke basis voor de gegevensverstrekking. Deze bepaling houdt in dat door de Nederlandse diensten, in het kader van het onderhouden van verbindingen met daarvoor in aanmerking komende inlichtingen- en veiligheidsdiensten van andere landen, aan deze instanties gegevens kunnen worden verstrekt ten behoeve van door deze instanties te behartigen belangen.

Uit de memorie van toelichting blijkt dat de twee vormen van gegevensverstrekking, op grond van artikel 59, tweede lid, Wiv 2002 en van artikel 36, eerste lid, Wiv 2002, van elkaar moeten worden onderscheiden. Verstrekking van gegevens op grond van artikel 36 Wiv 2002 vindt plaats in het kader van een goede taakuitvoering door de Nederlandse diensten, terwijl bij gegevensverstrekking op grond van artikel 59 Wiv 2002 het belang dat de buitenlandse dienst daarbij heeft leidend is. Bij gegevensverstrekking ingevolge artikel 59 Wiv 2002 staat het onderhouden van een goede samenwerkingsrelatie met de daarvoor in aanmerking

[249] *Kamerstukken II* 2000/01, nr. 14, p. 64.
[250] *Kamerstukken II* 2000/01, 25 877, nr. 14, p. 63.
[251] *Idem.*

komende buitenlandse dienst voorop.[252] Indien de AIVD of de MIVD gegevens heeft die voor een buitenlandse dienst van belang kunnen zijn, maar niet ingevolge artikel 36, eerste lid, sub d, Wiv 2002 verstrekt kunnen worden, kan de informatie – onder omstandigheden – aan de buitenlandse dienst worden verstrekt zonder dat dit bijdraagt aan de eigen taakuitvoering van de AIVD of de MIVD. Een buitenlandse dienst kan bijvoorbeeld verzoeken om informatie over een persoon of organisatie waar de AIVD of de MIVD zelf geen onderzoek naar doet. Wanneer de AIVD of de MIVD de gevraagde gegevens beschikbaar heeft, kan de dienst die gegevens verstrekken op grond van artikel 59, tweede lid, Wiv 2002. De verstrekking draagt in die gevallen niet bij aan een concreet lopend onderzoek van de Nederlandse dienst. In de meeste gevallen worden gegevens aan buitenlandse diensten echter verstrekt op grond van artikel 36 Wiv 2002.

Beide soorten gegevensverstrekking aan buitenlandse diensten vinden overigens plaats in het belang van de nationale veiligheid. Dit is evident waar het gaat om gegevensverstrekking in het kader van de uitvoering van de eigen taken van de diensten, maar ook bij gegevensverstrekking ten behoeve van het onderhouden van relaties met buitenlandse diensten, waarbij het belang van de buitenlandse dienst leidend is, geschiedt de verstrekking in het belang van de nationale veiligheid. Dit hangt nauw samen met het wederkerigheidsprincipe (*quid pro quo*). Samenwerking tussen diensten is geen eenzijdig proces. Niet alleen de AIVD en de MIVD kunnen van buitenlandse diensten informatie vragen die van belang is voor hun taakuitvoering, ook buitenlandse diensten kunnen het met het oog op hun activiteiten van belang achten bepaalde informatie van de Nederlandse diensten te verkrijgen. Dergelijke verzoeken dienen in beginsel positief tegemoet te worden getreden om ervan verzekerd te zijn dat dit – omgekeerd – ook gebeurt bij verzoeken van de AIVD en de MIVD.[253] Door het inwilligen van de verzoeken van bevriende buitenlandse diensten wordt, indirect, de eigen nationale veiligheid gediend, omdat op termijn een tegenprestatie verwacht kan worden indien daaraan behoefte bestaat.[254]

VI.2.2 Waarborgen

In de vorige paragraaf is een kader van waarborgen geschetst dat geldt voor de samenwerking met buitenlandse diensten. Hier wordt een aantal waarborgen dat specifiek betrekking heeft op (persoons)gegevensuitwisseling aan de orde gesteld.

Wanneer de AIVD dan wel de MIVD in een specifiek geval overweegt (persoons)gegevens te verstrekken aan een buitenlandse dienst, moet eerst worden bezien of deze vorm van samenwerking past binnen de algemene beoordeling van de desbetreffende dienst aan de hand van de eerdergenoemde algemene criteria. Hierbij dient te worden opgemerkt dat het op voorhand uitsluiten van iedere vorm van samenwerking met diensten die niet aan de samenwerkingscriteria voldoen desastreuze gevolgen zou kunnen hebben. Er dienen altijd communicatiekanalen open te blijven om informatie te ontvangen over acute, levensbedreigende situaties.

Op het verstrekken van gegevens aan buitenlandse diensten zijn de algemene regels over gegevensverwerking van toepassing. In beginsel geldt dus hetzelfde normenkader. De verstrekking dient te voldoen aan de algemene eisen van gegevensverwerking (artikel 12 Wiv 2002), dus onder meer voor een bepaald doel en slechts voor zover noodzakelijk voor

[252] *Kamerstukken II* 1999/2000, 25 877, nr. 8, p. 101.
[253] *Kamerstukken II* 1997/98, 25 877, nr. 3, p. 73; *Kamerstukken II* 1999/2000, 25 877, nr. 8. p. 101.
[254] *Kamerstukken I* 2001/02, 25 877, nr. 58a, p. 24

een goede uitvoering van de wet, en met inachtneming van de normen van behoorlijkheid en zorgvuldigheid. Wanneer de diensten op basis van artikel 36 Wiv 2002 gegevens verstrekken aan een buitenlandse dienst in het kader van hun eigen taakuitvoering, dan dient het in het belang van de nationale veiligheid noodzakelijk te zijn om de desbetreffende buitenlandse dienst op de hoogte te stellen van de te verstrekken informatie.

Voor de verstrekking van gegevens aan buitenlandse diensten op basis van artikel 59, tweede lid, Wiv 2002, waarbij het belang van de buitenlandse dienst leidend is, geldt dat de verstrekking noodzakelijk dient te zijn in het kader van het onderhouden van de verbinding met de desbetreffende buitenlandse dienst. Het onderhouden van verbindingen met buitenlandse diensten is, zoals hierboven gezegd, (indirect) in het belang van de nationale veiligheid. De Commissie merkt op dat de noodzakelijkheid van de gegevensverstrekking in het belang van de buitenlandse dienst al snel is gegeven door de zorgplicht van de Nederlandse diensten voor het onderhouden van verbindingen en het in de wetsgeschiedenis geformuleerde uitgangspunt dat verzoeken van bevriende diensten in beginsel positief tegemoet worden getreden.[255]

Het verstrekken van gegevens vindt doorgaans plaats op voorwaarde van de zogenoemde "derde partijregel" (*third party rule*), die inhoudt dat verkregen informatie slechts verder mag worden verstrekt als de dienst waarvan de informatie afkomstig is daarvoor toestemming heeft verleend (artikel 37 Wiv 2002). Volgens de wetsgeschiedenis vormt deze regel een essentiële voorwaarde bij internationale samenwerking:

> "Als een dienst er niet van op aan kan, dat een gegeven door de dienst in het geadresseerde land geheim wordt gehouden ten behoeve van de eigen informatiepositie kan er van werkelijke samenwerking tussen de betreffende diensten geen sprake zijn. Indien bij een dienst de indruk ontstaat dat deze regel niet wordt nageleefd, dan zal de informatie uitwisseling met die betreffende zusterdienst worden stopgezet of gemarginaliseerd."[256]

Door sommige inlichtingen- en/of veiligheidsdiensten wordt uitgegaan van de "derde *land*regel", waarbij een ruimere uitleg van deze internationale regel wordt gehanteerd. De verdere verstrekking van gegevens afkomstig van een buitenlandse dienst tussen de inlichtingen- en veiligheidsdiensten van hetzelfde land is ingevolge de derde landregel in beginsel toegestaan, tenzij dit uitdrukkelijk door de verstrekkende dienst wordt uitgezonderd.

De naleving van de *third party rule* vormt een belangrijke waarborg in de samenwerking tussen inlichtingen- en veiligheidsdiensten. Zo draagt de regel bij aan bronbescherming, de uitwisselbaarheid van geheime informatie en het wederzijdse vertrouwen dat de basis vormt voor een samenwerkingsrelatie tussen inlichtingen- en veiligheidsdiensten. Daarnaast zorgt de regel ervoor dat de verdere verstrekking van informatie gecontroleerd wordt. Hierdoor wordt de kans verkleind dat informatie afkomstig van één enkele bron bij meerdere partijen terechtkomt, die op hun beurt de informatie verder verstrekken, en het vervolgens lijkt alsof de informatie uit meerdere bronnen afkomstig is. De ongecontroleerde verdere verstrekking van informatie kan er tevens toe leiden dat opmerkingen van de verstrekkende dienst over de betrouwbaarheid van de informatie verloren gaan.

---

[255] *Kamerstukken I* 2001/02, 25 877, nr. 58a, p. 24.
[256] *Kamerstukken II* 1997/98, 25 877, nr. 3, p. 57.

De verstrekking van persoonsgegevens aan een buitenlandse dienst vormt een inbreuk op de persoonlijke levenssfeer van de betrokkene. Ten aanzien van de verstrekking van gegevens aan buitenlandse inlichtingen- en veiligheidsdiensten wordt in de wetsgeschiedenis onderscheid gemaakt tussen persoonsgegevens en andere gegevens. De verstrekking van persoonsgegevens dient met extra zorgvuldigheid te worden vormgegeven. Indien de AIVD of de MIVD persoonsgegevens wil verstrekken aan een dienst van een land waar twijfels kunnen bestaan over het respecteren van de mensenrechten, mogen deze persoonsgegevens slechts worden verstrekt indien en voor zover daarvoor een dringende noodzakelijkheid (onvermijdelijkheid) bestaat vanwege een onaanvaardbaar risico voor de maatschappij en haar burgers en waarbij snel handelen is vereist (bijv. onschuldige burgers dreigen het slachtoffer te worden van terroristische aanslagen).[257] Het verstrekken van persoonsgegevens aan buitenlandse diensten dient voorts schriftelijk te gebeuren (artikel 40 lid 1 Wiv 2002) en er dient aantekening van gehouden te worden (artikel 42 Wiv 2002).

VI.3 Ontvangen van gegevens

In het internationale verkeer tussen diensten en het daarbinnen geldende wederkerigheidsprincipe (*quid pro quo* oftewel "voor wat, hoort wat"), is het verkrijgen van gegevens van buitenlandse diensten in belangrijke mate verbonden met het verstrekken van gegevens door de AIVD en de MIVD. In de wetsgeschiedenis is opgemerkt dat het voor de AIVD of de MIVD om een zo compleet mogelijk beeld te kunnen krijgen met betrekking tot een bepaald onderwerp wenselijk is om een daarvoor in aanmerking komende dienst te kunnen vragen of hij eventueel informatie over het desbetreffende onderwerp heeft of, indien dat niet het geval is, zijn contacten kan gebruiken om alsnog aan informatie te komen. Zeker daarvoor in aanmerking komende inlichtingen- en/of veiligheidsdiensten uit de grotere landen beschikken volgens de wetgever over zulke gegevensverzamelingen en contacten dat zij voor de AIVD en de MIVD waardevolle informatie kunnen hebben.[258] De gegevens die door deze samenwerking worden verkregen, versterken in belangrijke mate de bestaande informatiepositie van de AIVD en de MIVD die daardoor beter in staat zijn om risico's voor de nationale veiligheid in te schatten en de verantwoordelijke autoriteiten hiervoor tijdig te waarschuwen.[259] Indien buitenlandse diensten over gegevens beschikken die bij kunnen dragen aan een goede taakuitvoering door de AIVD of de MIVD dan is het van belang dat deze gegevens ook kunnen worden verkregen.[260] De mogelijkheid om gegevens van buitenlandse diensten te verzoeken en te ontvangen is niet expliciet geregeld in de Wiv 2002, maar wordt verondersteld in artikel 59 Wiv 2002 dat ziet op het onderhouden van verbindingen met buitenlandse diensten. Een verzoek van een Nederlandse dienst aan een buitenlandse dienst dient evenwel te voldoen aan alle criteria die gelden voor gegevensverwerking.

Op grond van internationale mensenrechtenverdragen en de Grondwet dienen de AIVD en de MIVD zich bovendien te onthouden van het gebruik van informatie van buitenlandse diensten indien er concrete aanwijzingen bestaan dat deze door marteling is verkregen. Slechts in zeer uitzonderlijke noodsituaties mogen (of zelfs moeten) de diensten hiervan afwijken. In de praktijk blijkt het voor de diensten echter vrijwel onmogelijk om in concrete gevallen te achterhalen of informatie die afkomstig is van een buitenlandse inlichtingen- of veiligheidsdienst door foltering is verkregen. De reden hiervoor is dat inlichtingen- en

[257] *Kamerstukken II* 2000/01, 25 877, nr. 59, p. 16.
[258] *Kamerstukken II* 1997/98, 25 877, nr. 3, p. 73.
[259] *Idem*, p. 73-74.
[260] *Kamerstukken II* 1999/2000, 25 877, nr. 8, p. 101.

veiligheidsdiensten in hun onderlinge verkeer hun bronnen van informatie en werkwijze geheim houden. Bovendien zullen diensten nimmer stellen dat zij informatie door foltering hebben verkregen. Deze onzekerheid mag er echter niet toe leiden dat met bepaalde buitenlandse diensten elke vorm van samenwerking op voorhand volledig wordt uitgesloten. In dit verband is het bovendien des te meer van belang dat, voorafgaand aan de samenwerking met een buitenlandse inlichtingen- en/of veiligheidsdienst, zorgvuldig wordt gewogen in hoeverre de mensenrechtensituatie in een land aan samenwerking met de desbetreffende dienst van dat land in de weg staat. Eveneens zal de AIVD of de MIVD zich, naarmate de samenwerkingsrelatie voortduurt dan wel andere vormen aanneemt, telkens dienen af te vragen tot welk niveau de samenwerking met een dergelijke dienst kan strekken.[261]

Buitenlandse diensten verstrekken doorgaans gegevens op verzoek van de AIVD of de MIVD of op basis van daarover gemaakte afspraken. In de wetsgeschiedenis is overwogen dat buitenlandse diensten die voor de AIVD of de MIVD diensten verrichten, daarbij de voor hen geldende wet- en regelgeving in acht zullen moeten nemen. Dat geldt immers ook in de omgekeerde situatie. Dit houdt in dat het verwerven van gegevens door deze buitenlandse diensten in hun eigen land dient plaats te vinden met inachtneming van de voor hen geldende wettelijke kaders.[262] Hoewel de buitenlandse dienst een eigen verantwoordelijkheid heeft bij het beoordelen van een verzoek om gegevens van een Nederlandse dienst, betekent dit niet dat het de Nederlandse diensten vrij staat om elk verzoek dat zij wenselijk achten te richten aan buitenlandse diensten. Een verzoek om gegevens aan een buitenlandse dienst dient noodzakelijk te zijn in het kader van de eigen taakuitvoering van de Nederlandse dienst en dient te voldoen aan de normen van behoorlijkheid en zorgvuldigheid (artikel 12 Wiv 2002).

VI.4 Technische en andere vormen van ondersteuning

Naast de uitwisseling van gegevens vinden andere vormen van samenwerking plaats met buitenlandse diensten. Zo vindt operationele samenwerking plaats door het uitvoeren van gezamenlijke operaties waarbij veelal sprake is van de inzet van bijzondere bevoegdheden. Dit geschiedt (mede) in het kader van de eigen taakuitvoering van de Nederlandse diensten. Hiervoor gelden de algemene regels omtrent gegevensverwerking uit de Wiv 2002, waaronder de bepalingen omtrent de inzet van bijzondere bevoegdheden.

Artikel 59 Wiv 2002 voorziet in de mogelijkheid dat de AIVD en de MIVD in bepaalde gevallen samenwerken met andere diensten zonder dat de Nederlandse diensten hierbij hun eigen belangen dienen. In het kader van het onderhouden van relaties met buitenlandse inlichtingen- en veiligheidsdiensten mogen de Nederlandse diensten volgens artikel 59, vierde lid, Wiv 2002 aan buitenlandse diensten technische en andere vormen van ondersteuning verlenen ten behoeve van door deze diensten te behartigen belangen. Aan het verlenen van technische en andere vormen van ondersteuning worden vergelijkbare voorwaarden gesteld als aan het verstrekken van gegevens in het belang van de buitenlandse dienst. Ondersteuning mag slechts plaatsvinden voor zover de belangen die de buitenlandse dienst heeft te behartigen niet onverenigbaar zijn met de belangen die de Nederlandse dienst

---

[261] Voor een bespreking van dit onderwerp ten aanzien van de AIVD, zie het toezichtsrapport van de CTIVD nr. 22a inzake de samenwerking van de AIVD met buitenlandse inlichtingen- en/of veiligheidsdiensten, *Kamerstukken II* 2009/10, 29 924, nr. 39 (bijlage), paragraaf 5.1, beschikbaar op www.ctivd.nl.

[262] *Kamerstukken II* 2000/01, 25 877, nr. 14, p. 62.

heeft te behartigen (sub a) en voor zover een goede taakuitvoering door de Nederlandse dienst zich niet tegen de verlening van de ondersteuning verzet (sub b).

Als voorbeeld van het geval dat een goede taakuitvoering door de Nederlandse diensten zich verzet tegen het verlenen van ondersteuning aan een buitenlandse dienst wordt in de wetsgeschiedenis genoemd het frustreren van eigen lopende operaties van de AIVD of de MIVD. Tevens wordt opgemerkt dat ook de soort gewenste ondersteuning van belang is. Deze dient onder meer te passen binnen de juridische kaders die de diensten in acht moeten nemen. Indien een bepaalde vorm van ondersteuning zich daar niet mee verenigt, zou het wel verlenen van deze ondersteuning in strijd zijn met een goede taakuitvoering.[263]

Volgens de wetsgeschiedenis zullen verzoeken om ondersteuning naar verwachting veelal betrekking hebben op de uitoefening van bepaalde bijzondere bevoegdheden, zoals volg- en observatieacties. Hierbij dienen de voor de bijzondere bevoegdheden geldende wettelijke voorschriften in acht te worden genomen.[264] Dit betekent onder meer dat aan het noodzakelijkheidscriterium (artikel 18 Wiv 2002) door de AIVD of de MIVD voldaan dient te worden. Eveneens dient bij de verlening van ondersteuning door de inzet van bijzondere bevoegdheden voldaan te worden aan de vereisten van proportionaliteit en subsidiariteit, zoals neergelegd in de artikelen 31 en 32 Wiv 2002. De Commissie merkt op dat de noodzakelijkheid van de ondersteuning in het belang van de buitenlandse dienst al snel is gegeven door de zorgplicht van de Nederlandse diensten voor het onderhouden van verbindingen met daarvoor in aanmerking komende buitenlandse diensten en het in de wetsgeschiedenis geformuleerde uitgangspunt dat verzoeken van bevriende diensten in beginsel positief tegemoet worden getreden.[265] De Nederlandse dienst dient daarnaast de proportionaliteit en de subsidiariteit van de inzet van een bijzondere bevoegdheid in het kader van de ondersteuning af te wegen in de zin dat beoordeeld dient te worden of het middel in een evenredige verhouding staat tot het beoogde doel en of er niet volstaan kan worden met de inzet van een lichter middel.

Volgens artikel 59, vijfde en zesde lid, Wiv 2002 vindt het verlenen van ondersteuning alleen plaats met toestemming van de betrokken minister. Deze bevoegdheid kan de minister uitsluitend mandateren aan het hoofd van de dienst, voor zover het gaat om verzoeken met een spoedeisend karakter (bijvoorbeeld grensoverschrijdende volg- en observatieacties), waarbij geldt dat de minister van een verleende toestemming terstond wordt geïnformeerd. De bevoegdheid voor het geven van toestemming voor het verlenen van technische en andere vormen van ondersteuning is op dit (hoge) niveau neergelegd vanwege mogelijke politieke aspecten die aan het verlenen van ondersteuning verbonden kunnen zijn.[266] De uitvoering van de ondersteuning gebeurt vervolgens door de onder de minister ressorterende dienst en onder de verantwoordelijkheid van de betrokken minister.[267]

Elk zelfstandig optreden van een buitenlandse dienst op Nederlands grondgebied vormt een inbreuk op de Nederlandse soevereiniteit en vormt doorgaans een bedreiging voor de nationale veiligheid. Hierin is het belang van de Nederlandse diensten gelegen om tegen dergelijke praktijken handelend op te treden. Het is niet toegestaan buitenlandse diensten te

[263] *Kamerstukken II* 2000/01, 25 877, nr. 14, p. 64.
[264] *Kamerstukken II* 1999/2000, 25 877, nr. 9. p. 38.
[265] *Kamerstukken I* 2001/02, 25 877, nr. 58a, p. 24.
[266] *Kamerstukken II* 1999/2000, 25 877, nr. 8, p. 101 en nr. 9, p. 37.
[267] *Kamerstukken II* 1999/2000, 25 877, nr. 9, p. 38.

machtigen om zelfstandig op Nederlands grondgebied te opereren.[268] Buitenlandse diensten kunnen op Nederlands grondgebied alleen gelegitimeerd activiteiten ontplooien indien hiervoor toestemming is gegeven door de minister van BZK, dan wel het hoofd van de AIVD, en indien dit geschiedt onder supervisie en verantwoordelijkheid van deze dienst.[269] Voor zover het gaat om plaatsen in gebruik van het ministerie van Defensie ligt deze verantwoordelijkheid bij de minister van Defensie en de MIVD[270].[271]

De omgekeerde situatie is ook mogelijk: de AIVD of de MIVD kan een buitenlandse dienst verzoeken om (technische) ondersteuning te bieden. Voor zover buitenlandse diensten aan de AIVD of de MIVD ondersteuning verlenen zullen zij daarbij de voor hen geldende regelgeving in acht moeten nemen. De inzet van inlichtingenmiddelen door buitenlandse diensten op hun eigen grondgebied dient plaats te vinden met inachtneming van de voor hen geldende wettelijke kaders.[272] De mogelijkheid om ondersteuning te verzoeken aan een buitenlandse dienst is niet geregeld in de Wiv 2002. Dit laat onverlet dat de Nederlandse diensten niet zomaar elke vorm van ondersteuning aan een buitenlandse dienst mogen verzoeken. De Commissie heeft eerder geoordeeld dat een verzoek om ondersteuning aan een buitenlandse dienst voor een activiteit die in de Wiv 2002 als bijzondere bevoegdheid wordt aangemerkt, moet voldoen aan de daarvoor geldende vereisten van noodzakelijkheid, proportionaliteit en subsidiariteit.[273] Voorts is het niet toegestaan dat de Nederlandse diensten door middel van verzoeken aan buitenlandse diensten de Wiv 2002 en de daarin aan hen toegekende bijzondere bevoegdheden voor de verzameling van gegevens "omzeilen". Dit wordt ook wel aangeduid als een U-bochtconstructie. Zo mogen de Nederlandse diensten niet aan een buitenlandse dienst vragen om gegevens te verzamelen die zij zelf niet kunnen verkrijgen omdat de Wiv 2002 hen dat niet toestaat. Diensten mogen wel andere landen bevragen om hun eigen (technische) capaciteit aan te vullen. Daar is internationale samenwerking tussen diensten volgens de wetsgeschiedenis juist op gericht. In de Wiv 2002 en in de wetsgeschiedenis is niet uitdrukkelijk vastgelegd dat de diensten zich niet mogen bedienen van de zogenaamde U-bochtconstructie. Dit volgt echter wel uit de Wiv 2002 als geheel. In artikel 2 Wiv 2002 is immers opgenomen dat de diensten hun taken verrichten in gebondenheid aan de wet. Tevens voorziet de Wiv 2002 in een gesloten systeem van (bijzondere) bevoegdheden om gegevens te verzamelen en van (externe) verstrekking van deze gegevens. Hieruit volgt dat het de diensten niet is toegestaan om zich van inlichtingenmiddelen en methoden te bedienen die niet in de Wiv 2002 zijn geregeld, dus ook niet in het kader van de samenwerking met buitenlandse diensten.

Aldus vastgesteld in de vergadering van de Commissie d.d. 5 februari 2014.

---

[268] *Idem.*

[269] *Kamerstukken II* 2000/01, 25 877, nr. 14, p. 62-65; *Kamerstukken I* 2001/02, 25 877, nr. 58a, p. 25.

[270] De wet kent ook de mogelijkheid dat de MIVD bijzondere bevoegdheden uitoefent buiten plaatsen in gebruik van het ministerie van Defensie, mits toestemming daarvoor is verleend in overeenstemming met de minister van BZK. Zie paragraaf III.

[271] *Kamerstukken I* 2001/02, 25 877, nr. 58a, p. 25.

[272] *Kamerstukken II* 2000/01, 25 877, nr. 14, p. 62.

[273] Toezichtsrapport van de CTIVD nr. 22a inzake de samenwerking van de AIVD met buitenlandse inlichtingen- en/of veiligheidsdiensten, *Kamerstukken II* 2009/10, 29 924, nr. 39 (bijlage), paragraaf 2.2, beschikbaar op www.ctivd.nl.