COMMISSIE VAN TOEZICHT
BETREFFENDE
DE INLICHTINGEN- EN VEILIGHEIDSDIENSTEN

TOEZICHTSRAPPORT

inzake
onderzoek door de AIVD op sociale media

CTIVD nr. 39

[16 juli 2014]

COMMISSIE VAN TOEZICHT
BETREFFENDE
DE INLICHTINGEN- EN VEILIGHEIDSDIENSTEN

CTIVD nr. 39

TOEZICHTSRAPPORT

inzake onderzoek door de AIVD op sociale media

Inhoudsopgave

COMMISSIE VAN TOEZICHT
BETREFFENDE
DE INLICHTINGEN- EN VEILIGHEIDSDIENSTEN

CTIVD nr. 39

Begrippenlijst

Bij het toezichtsrapport
inzake onderzoek op sociale media door de AIVD

In deze lijst wordt een aantal begrippen toegelicht zoals deze gebruikt worden in dit toezichtsrapport. 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.

Acquisiteur	Medewerker van de dienst die het contact met menselijke bronnen (informanten en agenten) onderhoudt.
Agent	Een persoon die gericht door de dienst wordt ingezet om gegevens te verzamelen (artikel 21 Wiv 2002). Een agent werkt onder aansturing en onder supervisie van de dienst.
Algemene bevoegdheid	De bevoegdheid van de AIVD tot het verzamelen van gegevens (artikelen 12 en 17 van de Wiv 2002). De AIVD mag deze bevoegdheid voor alle in artikel 6 genoemde taken gebruiken. De algemene bevoegdheid moet worden onderscheiden van de bijzondere bevoegdheden (zie hierna).
Bevraging	Het (persoons)gericht bevragen van een aanbieder of buitenlandse dienst die toegang heeft tot een gegevensverzameling van sociale media.
Bewerker	De bewerker is de medewerker die onder meer nieuwe gegevens beoordeelt en op basis daarvan de aanzet doet voor inlichtingenproducten, de koers van het team en de eventuele inzet van bevoegdheden.
Bijzondere bevoegdheid	Een bevoegdheid van de dienst die een specifieke inbreuk op de persoonlijke levenssfeer maakt. De toepassing van een bijzondere bevoegdheid heeft veelal een geheim karakter. De bijzondere bevoegdheden en de voorwaarden waaronder deze mogen worden toegepast zijn neergelegd in de artikelen 20 t/m 30 van de Wiv 2002 (bijvoorbeeld tappen of hacken).
Cyber	Datgene dat samenhangt met de digitale of virtuele wereld, waaronder het internet.
Directeur (AIVD)	Functionaris binnen de dienst die hiërarchisch als volgt is ingebed in de organisatie: hoofd, *directeur,* unithoofd, teamhoofd.
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 (artikel 29 Wiv 2002).
Geëvalueerde gegevens	Gegevens die op relevantie zijn beoordeeld.
Gefingeerde identiteit	Het geheel van persoonskenmerken waarmee iemand zich presenteert als een ander, niet-bestaand persoon. Ook wel 'dekmantel' genoemd in de zin van artikel 21 Wiv 2002.
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 en onder f, van de Wiv 2002). Het enkele *verzamelen* van gegevens wordt wel aangeduid als gegevensverwerving.
Gegevensverzameling	Verzameling van gegevens. Deze kan door de AIVD zijn samengesteld, maar kan ook worden verkregen uit open bronnen, door de inzet van (bijzondere) bevoegdheden of van externe partijen.
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 verwerven (artikel 24 Wiv 2002). Een hack kan worden uitgevoerd op afstand (bijvoorbeeld via het internet) of als de dienst het apparaat onder zich heeft (bijvoorbeeld door het wachtwoord van een laptop die de dienst in handen heeft te ontcijferen).
Hoofd (AIVD)	Functionaris die de leiding heeft over de dienst. De hiërarchische inbedding in de organisatie is als volgt: *hoofd*, directeur, unithoofd, teamhoofd.
Informant	Een persoon of instantie tot wie de dienst zich kan wenden om gegevens te verzamelen (artikel 17 Wiv 2002). Een informant wordt niet aangestuurd en wordt geacht vanuit zijn gebruikelijke activiteiten informatie te kunnen verstrekken.
Inlichtingentaak (AIVD)	Het doen van onderzoek naar andere landen (zie artikel 6, tweede lid, aanhef en onder d, van de Wiv 2002).
Interceptie	Het onderscheppen van gegevens.
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 inzetten van een telefoontap heeft de dienst bijvoorbeeld een last van de minister nodig).
Mandaatbesluit	Mandaatbesluit bijzondere bevoegdheden 2009, vastgesteld door het hoofd van de AIVD. Dit besluit is niet gepubliceerd.
Menselijke bron	Informant of agent.
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.
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 een technisch kenmerk zoals een telefoonnummer) van de contacten van een target met andere personen en de contacten van die personen met weer andere personen.
Nickname	Een door een internetgebruiker (bijvoorbeeld op sociale media) opgegeven naam, waarmee hij of zij zich naar anderen presenteert.
Ondersteunend team	Een team dat geen (inhoudelijk) onderzoek verricht naar één van de aandachtsgebieden van de AIVD, maar veelal op verzoek van operationele teams bijzondere bevoegdheden inzet, of daaromtrent adviseert. Zo kan een operationeel team een ondersteunend team verzoeken een hack in te zetten op een bepaald target, omdat bij het ondersteunende team de expertise daartoe aanwezig is. Het ondersteunde team gebruikt de gegevens die de hack oplevert zelf niet.
Ongerichte interceptie	Als niet van tevoren kan worden aangegeven op welke persoon, organisatie of technisch kenmerk de interceptie gericht is.
Ontsluiting	Het toegankelijk of doorzoekbaar maken van gegevens.
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.
Operationeel team	Een team dat onderzoek verricht naar één van de aandachtsgebieden van de AIVD. Dit kan bijvoorbeeld een team zijn dat onderzoek doet naar terrorisme.
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).
Platform	Een bepaalde vorm of toepassing van sociale media.
Ruwe gegevens	Gegevens verkregen door middel van de inzet van (bijzondere) bevoegdheden die nog niet op relevantie zijn beoordeeld. Ook wel *ongeëvalueerde* gegevens genoemd.
Select before you collect	Het uitgangspunt dat de AIVD slechts gegevensverzamelingen zal verwerven indien de dienst in staat is deze effectief te bewerken.
Stromende telecommunicatie /transport fase	Stromende informatie is 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.
Teamhoofd (AIVD)	Functionaris binnen de dienst die hiërarchisch als volgt is ingebed in de organisatie: hoofd, directeur, unithoofd, *teamhoofd*.
Telecommunicatie	Communicatie over afstand door middel van elektronische middelen (bijvoorbeeld telefoon, radio, fax en internet).
Unithoofd (AIVD)	Functionaris binnen de dienst 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 nationale veiligheid of voor andere gewichtige belangen van de staat, dan wel voor de veiligheid en de paraatheid van de krijgsmacht.
Veiligheidsonderzoek	Onderzoek op grond van artikel 7 van de Wet op de veiligheidsonderzoeken naar een persoon die een vertrouwensfunctie vervult of gaat vervullen waarin hij of zij de nationale veiligheid kan schaden.
Veiligheidstaak (AIVD)	Taak gericht op het onderkennen van dreigingen voor het voortbestaan van de democratische rechtsorde dan wel voor de veiligheid of voor andere gewichtige belangen van de staat (artikel 6, tweede lid, aanhef en onder a, van de Wiv 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 Wiv 2002).
Verwervende of ondersteunende afdeling	De afdeling binnen de AIVD 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 ten behoeve waarvan een bijzondere bevoegdheid wordt ingezet.
Webforum	Discussiepagina op het internet. Op sommige webfora dienen bezoekers zich aan te melden om toegang te krijgen. Via deze pagina's kunnen de bezoekers veelal ook onderling berichten uitwisselen.

CTIVD nr. 39

Samenvatting

Van het toezichtsrapport
inzake onderzoek op sociale media door de AIVD

Sociale media spelen in de huidige tijd een grote rol in het maatschappelijk verkeer. Voor de AIVD zijn sociale media mede daardoor een belangrijke bron van inlichtingen geworden. Vanwege de omvang van de communicatie op sociale media en de lage drempel om hieraan deel te nemen zijn berichten niet altijd snel te duiden: is een dreigtweet een wanhopige uiting van een boze tiener of een serieuze aanwijzing voor verregaande radicalisering? De maatschappij mag van de AIVD verwachten dat de dienst adequaat inspeelt op de ontwikkelingen op sociale media bij de uitvoering van zijn taken. De Commissie heeft in dit onderzoek bezien of de AIVD bij deze activiteiten rechtmatig te werk gaat.

Gelet op de taak van de AIVD is van belang dat geheim blijft naar wie precies wordt gekeken en op welke manier dit gebeurt. Deze geheimhouding geeft ruimte aan speculatie, zeker sinds in 2013 informatie naar buiten is gekomen over de activiteiten van enkele buitenlandse diensten. In relatie tot de AIVD ging het in de media en publieke discussies veelal om de volgende vragen:

- hoe gebruikt de AIVD sociale media?
- wat mag de AIVD in verband met sociale media en respecteert de AIVD de wet?
- wat doet de AIVD met de gegevens die op sociale media worden verzameld?
- hoe werkt de AIVD hierbij samen met buitenlandse diensten?

De Commissie heeft aan de hand van feiten- en dossieronderzoek bij de AIVD en uitgaande van de kaders die de Wet op de inlichtingen- en veiligheidsdiensten (Wiv 2002) stelt, bovenstaande vragen meegenomen in dit onderzoek. Het onderzoek heeft zich toegespitst op de periode van 1 januari 2011 tot 1 januari 2014.

Toen de Wiv 2002 werd geschreven, nam internet nog niet de plaats in die het tegenwoordig heeft en waren sociale media nog in opkomst. Het toepassen van 'klassieke' bevoegdheden in die 'nieuwe' digitale context, zoals het inzetten van agenten en observatie op internet, dwingt de AIVD na te denken over hoe de nationale veiligheid moet worden geborgd in relatie tot de bescherming van de privacy en de wettelijke waarborgen daarvoor. De dienst moet immers bij de uitvoering van zijn taken strikt binnen de wet opereren. Dit betekent onder meer dat iedere inbreuk op de privacy een grondslag in de wet dient te hebben en dat alleen een inbreuk mag worden gemaakt wanneer dit noodzakelijk is. Deze inbreuk moet in een redelijke verhouding staan tot het te dienen doel en er moeten geen lichtere middelen voorhanden zijn. Bij het ontwikkelen van nieuwe technieken dient de AIVD zich hiervan voortdurend bewust te zijn en principiële vragen moeten tijdig worden onderkend.

De Commissie constateert dat de Wiv 2002 op de meeste punten een voldoende kader biedt om de rechtmatigheid op het gebruik van sociale media te beoordelen. Daarnaast signaleert de Commissie dat de AIVD veel inspanningen onderneemt om de technische

ontwikkelingen op het vlak van sociale media bij te houden. Het beleid van de dienst waarin de waarborgen voor de bescherming van de persoonlijke levenssfeer zijn neergelegd, is echter op sommige punten achtergebleven bij die ontwikkeling. Met name het motiveren van de inzet van bevoegdheden en de verslaglegging van de operaties (instructies, opbrengst) blijft achter bij hetgeen van een rechtmatig opererende dienst mag worden verwacht. De Commissie begrijpt dat in de pioniersfase nog niet onmiddellijk duidelijk was hoe deze essentiële waarborgen een vaste plaats dienden te krijgen in de werkwijzen.Maar inmiddels is de AIVD de fase van het pionieren voorbij en mag worden verwacht dat de toegepaste methoden zijn ingebed in bestendige procedures.

De interactie tussen gebruikers van sociale media vindt gedeeltelijk plaats in het publieke domein. Net als eenieder kan de AIVD daar ook kennis van nemen. De AIVD mag deze gegevens op grond van zijn *algemene bevoegdheid* verzamelen. Een belangrijke grens aan het verzamelen van deze gegevens is de mate van de inbreuk op de privacy. Zodra een activiteit een inbreuk inhoudt, moet daarvoor een specifieke wettelijke grondslag aanwezig zijn. Ook moet deze activiteit in toenemende mate met waarborgen zijn omgeven naar gelang de inbreuk zwaarder wordt. De Commissie heeft bij haar onderzoek naar het verzamelen van gegevens op basis van de algemene bevoegdheden geen onrechtmatigheden aangetroffen.

Vanwege de zwaarte van de inbreuk op de privacy is in dit onderzoek vooral aandacht besteed aan enkele heimelijke *bijzondere bevoegdheden,* waaronder de inzet van agenten. Op sociale media vindt communicatie plaats die relevant is voor de taakuitvoering door de AIVD. De dienst speelt hierop in door agenten in te zetten op deze media. Deze mogen zich hierbij van een gefingeerde identiteit bedienen. Ook mogen de agenten, onder strikte voorwaarden, strafbare feiten plegen om bijvoorbeeld niet uit de toon te vallen binnen de kring waar ze worden ingezet.

De Commissie heeft verschillende agentenoperaties bestudeerd. Waar het *externe* agenten betreft is zij van oordeel dat de AIVD zorgvuldig en doordacht te werk gaat. Waar het *eigen* medewerkers betreft schieten de operaties echter regelmatig tekort op het vlak van verslaglegging. In vijf agentenoperaties waarbij medewerkers van de AIVD zijn ingezet op sociale media onder een virtuele identiteit, is het gebrek aan verslaglegging van dien aard dat de Commissie van oordeel is dat die operaties op dit punt op onrechtmatige wijze zijn uitgevoerd. Ten behoeve van de veiligheid van de agenten, de interne verantwoording en het extern toezicht door de Commissie is verslaglegging van wezenlijk belang. Het gebrek aan verslaglegging doet zich ook voor in operaties waarin een toestemming is gegeven om strafbare feiten te plegen. De Commissie is van oordeel dat hierdoor ook aan deze toestemming op onrechtmatige wijze uitvoering is gegeven. Door de gebrekkige verslaglegging is niet na te gaan of de agenten zich aan hun instructies hebben gehouden en in hoeverre voldoende sturing aan hen is gegeven. Recent echter heeft de AIVD een aantal problemen bij de begeleiding en ondersteuning van de online opererende medewerkers onderkend en is een verbetertraject ingezet.

Aanbieders van sociale media slaan vaak metagegevens of de inhoud van communicatie op in gegevensverzamelingen. Dit gebeurt ook bij webfora. De AIVD kan via verschillende wegen (target)gerichte bevragingen uitvoeren op dergelijke gegevensverzamelingen. Wanneer dit noodzakelijk is voor de taken, en dit voldoet aan de beginselen van proportionaliteit en subsidiariteit, mag de AIVD ook proberen de gehele gegevensverzameling te verwerven. Dit kan op uiteenlopende manieren, bijvoorbeeld via een menselijke bron, een hack of een buitenlandse dienst. Naarmate de verzameling algemener van aard is, kan worden gezegd dat de verwerving meer ongericht van karakter

is. In dat geval gelden naar het oordeel van de Commissie strengere eisen aan de voorafgaande motivering, te weten een verzwaarde proportionaliteitstoets. In die gevallen worden namelijk ook gegevens van personen verzameld die niet relevant zijn voor de taakuitvoering door de dienst.

De Commissie is van oordeel dat de motiveringen voor het verwerven van een groot aantal webfora tekortschieten. Ten aanzien van vijf agentenoperaties waarbij webfora zijn verworven, is de Commissie van oordeel dat de motivering van de inzet van deze agenten dermate tekortschiet dat de toestemmingen hiervoor onrechtmatig zijn gegeven. In de meeste gevallen is de Commissie er overigens wel van overtuigd dat de verwerving van deze webfora noodzakelijk was en past binnen de taakstelling van de dienst. In vier (andere dan de hiervoor genoemde) gevallen vindt de Commissie echter de verwerving van bepaalde webfora niet proportioneel en is zij van oordeel dat de verwerving om die reden onrechtmatig was. Het ging hierbij om grotere webfora waarbij de te verwachten opbrengst in geen verhouding stond tot de inbreuk op de persoonlijke levenssfeer van die gebruikers van de webfora op wie lopende onderzoeken niet gericht waren.

De AIVD mag gegevens die door middel van de inzet van bijzondere bevoegdheden voor de veiligheids- of inlichtingentaak zijn verzameld ook gebruiken voor andere taken, zoals de uitvoering van veiligheidsonderzoeken. De Commissie is van oordeel dat dit alleen geldt voor *geëvalueerde* gegevens; gegevens die na (metadata)analyse daadwerkelijk relevant zijn gebleken voor een operationeel onderzoek. Het toegankelijk maken van *ongeëvalueerde* (ruwe) gegevens van webfora ten behoeve van veiligheidsonderzoeken beoordeelt zij als onrechtmatig. De wet biedt hier geen toereikende grondslag voor.

Zoals de Commissie reeds in een eerder toezichtsrapport heeft opgemerkt, schrijft de wet geen bewaartermijn voor ongeëvalueerde (ruwe) gegevens voor. De Commissie beveelt de AIVD aan, vooruitlopend op een mogelijke wetswijziging, zelf bewaartermijnen vast te stellen. In dit onderzoek is bezien of de verworven webfora op goede gronden worden bewaard. De Commissie is van oordeel dat de AIVD de bestudeerde webfora, voor zover rechtmatig verworven, heeft mogen bewaren.

Omdat de communicatie via sociale media nauwelijks gebonden is aan landsgrenzen, raken de onderzoeken van de AIVD in verband met sociale media vaak aan de belangen en de rechtsordes van andere landen. Enerzijds zijn de targets van de dienst veelal internationaal actief. Anderzijds brengt het opereren in een online context, bijvoorbeeld door een agent van de AIVD, met zich mee dat vaak gegevens worden verzameld die (ook) relevant zijn voor andere landen. Het wederzijdse belang bij samenwerking kan nauwelijks overschat worden. Webfora kunnen zeer grote hoeveelheden gegevens bevatten die niet alleen voor Nederland van belang zijn. De Commissie benadrukt het belang van goede afspraken met buitenlandse diensten teneinde het risico te beperken dat relevante gegevens over het hoofd worden gezien.

De Commissie heeft geen aanwijzingen dat de AIVD bij de samenwerking met buitenlandse diensten de eigen bevoegdheden omzeilt. Voorts heeft de Commissie ten aanzien van operaties die de AIVD samen met buitenlandse diensten heeft uitgevoerd geen onrechtmatigheden geconstateerd. Hier wordt over het algemeen zorgvuldig en bedachtzaam te werk gegaan, en hiervan wordt in voldoende mate verslag bijgehouden.

Tot slot heeft de Commissie bijzondere aandacht besteed aan het delen van door de AIVD verworven webfora met buitenlandse diensten. In vrijwel alle onderzochte gevallen heeft de

AIVD hierbij rechtmatig gehandeld. Op dat algemene beeld zijn de volgende uitzonderingen vastgesteld. De AIVD heeft een aantal webfora verworven op verzoek van specifieke buitenlandse diensten. Als een webforum voor een buitenlandse dienst wordt verworven terwijl dat forum niet van belang is voor een lopend onderzoek van de AIVD, is sprake van het verlenen van ondersteuning aan de buitenlandse dienst. De wet schrijft voor dat in dat geval toestemming aan de minister moet worden gevraagd voordat de gegevens worden verworven. Nu de toestemming van de minister ontbrak, is naar het oordeel van de Commissie in vier gevallen onrechtmatig gehandeld. In een vijfde geval heeft de AIVD een webforum gedeeld met een buitenlandse dienst waarvan de Commissie de verwerving door de AIVD niet proportioneel achtte. Het verwerven en vervolgens delen van dit forum geschiedde dan ook onrechtmatig.

COMMISSIE VAN TOEZICHT
BETREFFENDE
DE INLICHTINGEN- EN VEILIGHEIDSDIENSTEN

CTIVD nr. 39

Toezichtsrapport

inzake onderzoek op sociale media door de AIVD

1. Inleiding

De Algemene Inlichtingen- en Veiligheidsdienst (AIVD) wint in het kader van zijn inlichtingen- en veiligheidstaken gegevens in uit diverse bronnen. Het internet heeft als bron van informatie het afgelopen decennium aanzienlijk aan betekenis gewonnen. Evenals in de niet-virtuele wereld ontmoeten mensen elkaar immers op het internet. Er wordt gediscussieerd, er worden ideeën uitgewisseld en er worden nieuwe contacten gelegd. Het kan hier gaan om het digitale equivalent van het publieke domein (de openbare ruimte) of om meer private omgevingen. De online platformen waarop individuen kunnen communiceren, in besloten kring of in het digitale publieke domein, worden tezamen wel aangeduid als sociale media. De AIVD kan relevante gegevens op sociale media op verschillende wijzen verzamelen. Zo kan de dienst de bevoegdheden tot tappen en hacken inzetten, maar ook zonder gebruikmaking van technische middelen kan de dienst gegevens inwinnen.

In haar toezichtsrapport inzake de afwegingsprocessen van de AIVD met betrekking tot Mohammed B., merkte de Commissie op dat de AIVD in 2004 nog geen goede informatiepositie op het internet had. Voorts stelde de Commissie "dat van een inlichtingen- en veiligheidsdienst mag worden verwacht dat ontwikkelingen van nieuwe communicatiemiddelen op de voet worden gevolgd en dat daar (snel) op wordt ingespeeld."[1] Blijkens de opvolgende openbare jaarverslagen sinds 2004 heeft de AIVD nadien sterk geïnvesteerd op het onderzoek in verband met internet, waaronder ook sociale media. De dienst heeft meermalen de dreiging van het jihadistisch internet afzonderlijk onder de aandacht gebracht.[2]

In dit diepteonderzoek is bezien of de inspanningen op het terrein van sociale media als rechtmatig kunnen worden beoordeeld.

De Commissie heeft dit onderzoek verricht op grond van de toezichthoudende taak die artikel 64 van de Wet op de inlichtingen- en veiligheidsdiensten 2002 (Wiv 2002) aan haar opdraagt. Een vooronderzoek is op 1 mei 2013 aangevangen. Op 2 oktober 2013 is het voornemen tot het onderzoek aangekondigd aan de minister van Binnenlandse Zaken en Koninkrijksrelaties en de voorzitters van de Eerste en Tweede Kamers der Staten-Generaal.

---

[1] Toezichtsrapport van de CTIVD nr. 17 inzake afwegingsprocessen van de AIVD met betrekking tot Mohammed B., *Kamerstukken II* 2007/08, 29 854, nr. 22 (bijlage), paragraaf 7.4. Alle toezichtsrapporten van de Commissie zijn te raadplegen op: www.ctivd.nl.

[2] De AIVD besteedt in de jaarverslagen hier aandacht aan, alsmede via losse publicaties: *De gewelddadige jihad in Nederland – Actuele trends in de islamitische-terroristische dreiging* (2006), en *Het jihadistisch internet – Kraamkamer van de hedendaagse jihad* (2012).

De Commissie heeft haar onderzoek op 5 maart 2014 afgerond en het toezichtsrapport opgesteld op 18 maart 2014. De minister van Binnenlandse Zaken en Koninkrijksrelaties is conform artikel 79 Wiv 2002 in de gelegenheid gesteld te reageren op de in het toezichtsrapport opgenomen bevindingen. De reactie van de minister is op 28 april 2014 door de Commissie ontvangen. De reactie op het toezichtsrapport heeft de Commissie aanleiding gegeven op enkele punten nader onderzoek te doen, alvorens het rapport vast te stellen. Daarnaast heeft een aanvullend gesprek met een medewerker van de AIVD plaatsgevonden. Dit alles heeft ertoe geleid dat het toezichtsrapport op enkele onderdelen is aangepast. De Commissie merkt op dat, mede als gevolg van de aanvullende onderzoeksactiviteiten, sprake is geweest van enig tijdsverloop tussen de reactie van de minister en het vaststellen van het toezichtsrapport op 16 juli 2014.

2. Opzet van het onderzoek

Sinds medio 2013 is de publieke aandacht voor de werkwijzen van de inlichtingendiensten in het algemeen sterk toegenomen. De Commissie heeft zich bij de opzet van dit onderzoek rekenschap gegeven van de vragen die leven in de samenleving. Ten aanzien van sociale media begrijpt de Commissie dat het vooral om de volgende vragen gaat:

- hoe gebruikt de AIVD sociale media?
- wat mag de AIVD in verband met sociale media en respecteert de AIVD de wet?
- wat doet de AIVD met de gegevens die op sociale media verzameld worden?
- hoe werkt de AIVD hierbij samen met buitenlandse diensten?

In verband met de publieke discussie heeft de Commissie in maart 2014 een rapport uitgebracht over gegevensverwerking op het gebied van telecommunicatie.[3] In dat rapport heeft de Commissie de toezegging gedaan nader onderzoek te doen naar bepaalde werkwijzen van de AIVD, te weten het hacken door menselijke bronnen, het hacken van webfora en het bewaren en uitwisselen van webfora. Ook signaleerde de Commissie in dat rapport onder meer dat nieuwe technische mogelijkheden en digitalisering van de samenleving ertoe hebben geleid dat bestaande bevoegdheden op een wijze kunnen worden ingezet die bij de totstandkoming van de wet nog niet werd voorzien. Met onderhavig onderzoek doet de Commissie deze toezegging gestand en heeft zij in het bijzonder bekeken of het onderzoek door de AIVD op sociale media in concrete operaties in lijn is met de bescherming van de persoonlijke levenssfeer.

De Commissie heeft zich met dit diepteonderzoek een breed beeld willen vormen van de activiteiten die de dienst ontplooit op het terrein van sociale media. Daartoe zijn de relevante beleidsdocumenten en de activiteiten van twee operationele teams op dit vlak nader bestudeerd. Een van deze teams doet reeds sinds lange tijd intensief onderzoek op sociale media, terwijl voor het andere team sociale media slechts één van de vele bronnen is waaruit het team gegevens verzamelt.[4] Hierbij is ook gekeken naar de activiteiten van het

[3] Toezichtsrapport van de CTIVD nr. 38 inzake gegevensverwerking op het gebied van telecommunicatie door de AIVD en de MIVD, *Kamerstukken II* 2013/14, 29 924, nr. 105 (bijlage). Hierna aangehaald als: toezichtsrapport nr. 38 van de CTIVD.

[4] Ter bescherming van bronnen en het actuele kennisniveau van de AIVD wordt in dit toezichtsrapport in het midden gelaten op welke aandachtsgebieden deze operationele teams zich richten. De AIVD doet van het werk van deze teams in het openbaar verslag via het jaarverslag.

ondersteunende team, onder meer gericht op de verwerving van webfora. De Commissie heeft hiertoe diepgaand dossieronderzoek gedaan naar enige tientallen operaties en heeft met dertien medewerkers op sleutelfuncties diverse gesprekken gevoerd. Door deze opzet heeft de Commissie een representatief beeld verkregen van het operationeel gebruik van sociale media door de AIVD.

Het verzamelen van gegevens op sociale media kan op meerdere wijzen geschieden. Bij dit diepteonderzoek is gekeken naar de menselijke dimensie van gegevensverwerving op sociale media. De inzet van technische middelen, zoals tappen en de selectie van sigint is of wordt door de Commissie reeds in andere diepteonderzoeken onderzocht.[5] De bevoegdheid van artikel 24 om een geautomatiseerd werk binnen te dringen (hacken) is in dit onderzoek betrokken waar deze bevoegdheid is gebruikt om gegevensverzamelingen van sociale media te verwerven. Dit houdt in dat in het bijzonder is gekeken naar de verwerving en verwerking van webfora.

Het dossieronderzoek heeft zich toegespitst op de periode vanaf 1 januari 2011 tot 1 januari 2014. Hiervoor is gekozen om binnen een redelijke termijn tot een rapport te kunnen komen, maar ook omdat is gebleken dat de ontwikkelingen op het vlak van (het onderzoek op) sociale media elkaar de afgelopen jaren snel hebben opgevolgd. Conclusies over eerdere periodes zouden slechts beperkte waarde hebben voor de huidige praktijk van de AIVD. Met betrekking tot de bestudeerde webfora tekent de Commissie aan dat het in enkele gevallen om grote gegevensverzamelingen gaat. Door middel van steekproeven en naslagen in de documentatiesystemen van de AIVD, heeft de Commissie getracht zich een zo volledig mogelijk oordeel te vormen van deze gegevensverzamelingen.

Dit rapport is als volgt opgezet. Paragraaf 3 gaat kort in op de definitie en werking van sociale media. Paragraaf 4 beschrijft het wettelijk kader. Hierin wordt het kader dat de Commissie heeft beschreven in het toezichtsrapport nr. 38 en de bijbehorende juridische bijlage nader uitgewerkt en toegespitst op sociale media. In paragraaf 5 worden de bestaande methoden om van sociale media gegevens te verzamelen nader geduid en worden de bevindingen van de Commissie over concrete operaties aangegeven. Hierbij is met name gekeken naar de mate van de inbreuk op grondrechten en de rechtvaardiging hiervoor, alsmede naar een aantal aspecten van de operationele uitvoering, zoals verslaglegging, aansturing en veiligheid. Tot slot volgen in paragraaf 6 de conclusies en aanbevelingen van de Commissie.

Dit rapport heeft een geheime bijlage. In deze bijlage worden ten aanzien van de geconstateerde onrechtmatigheden geen conclusies getrokken die niet ook in het openbare gedeelte van dit rapport worden vermeld. Tevens heeft het openbare gedeelte een bijlage waarin het toetsingskader beknopt wordt weergegeven.

[5] Vervolgonderzoeken door de CTIVD naar de inzet van de afluisterbevoegdheid en van de bevoegdheid tot de selectie van sigint door de AIVD: toezichtsrapport nr. 31 over de periode september 2010 t/m augustus 2011, *Kamerstukken II* 2012/13, 29 924, nr. 86 (bijlage); toezichtsrapport nr. 35 over de periode september 2011 t/m augustus 2012, *Kamerstukken II* 2013/14, 29 924, nr. 101 (bijlage); lopend onderzoek over de periode september 2012 t/m augustus 2013: wordt naar verwachting in september 2014 gepubliceerd.

3. Het begrip sociale media

Er zijn veel definities van het fenomeen sociale media in omloop. Binnen de AIVD is de volgende definitie in gebruik, die ook in het kader van dit toezichtsrapport wordt gehanteerd:

> "Sociale media is een verzamelnaam voor toepassingen die gebruik maken van het internet en als doel hebben om individuele gebruikers door middel van een mix van verschillende media (tekst, foto, video) bewust en/of onbewust publieke en private interactie aan te laten gaan met andere gebruikers van die toepassingen."

Hierbij is het van belang te wijzen op het onderscheid tussen het open en afgeschermde gedeelte van sociale media. Veel van wat op sociale media gebeurt, is voor iedere internetgebruiker waarneembaar en eenvoudig te vinden via zoekmachines zoals Google. In verschillende gradaties kan een gebruiker of aanbieder de communicatie echter afschermen, bijvoorbeeld door de toegang tot leden te beperken, zoals de aanbieder LinkedIn doet, of doordat de gebruiker bepaalt wie wat kan zien. Zo kan de gebruiker op Facebook beperken hoeveel de buitenwereld ziet van zijn informatie en op een webforum kunnen open en afgeschermde discussiegroepen naast elkaar bestaan. Ook kunnen via veel platformen berichten direct naar een andere gebruiker worden gestuurd, wat te vergelijken is met e-mail of sms.

Terwijl een kenmerkend element van sociale media is dat individuele gebruikers de inhoud vormgeven, slaan de bedrijven en instellingen die sociale media ontwikkelen en aanbieden veelal de inhoud en metagegevens van de communicatie op. Dit betekent dat er (grote) gegevensverzamelingen bestaan in verband met sociale media.

In dit toezichtsrapport wordt gesproken van onderzoek *op* sociale media, wanneer de AIVD zich als het ware mengt tussen de individuele gebruikers op sociale media en in sommige gevallen hieraan actief deelneemt. Er wordt gesproken van onderzoek *aan* gegevens van sociale media wanneer het gaat om de gegevensverzamelingen die bestaan bij de aanbieders van de verschillende platformen. Tezamen worden deze vormen van onderzoek wel aangeduid als *social media intelligence* (socmint).[6]

4. Wettelijk kader

In het recente toezichtsrapport inzake gegevensverwerking op het gebied van telecommunicatie heeft de Commissie in de juridische bijlage uitgebreid de wettelijke kaders uiteengezet waarbinnen de AIVD en de Militaire Inlichtingen- en Veiligheidsdienst (MIVD) dienen te werken.[7] In het bestek van dit rapport is er daarom voor gekozen het wettelijk kader slechts uit te diepen voor zover dit een bijzondere betekenis of invulling heeft in de context van sociale media. In de bijlage bij dit toezichtsrapport wordt een overzicht gegeven van het toetsingskader in relatie tot de door de dienst toegepaste onderzoeksmethoden op sociale media.

[6] Ontleend aan: D. Omand, J. Bartlett en C. Miller, #*Intelligence*. Londen: Demos, 2012.
[7] Toezichtsrapport nr. 38 van de CTIVD.

4.1 Mensenrechtelijk kader

Wanneer een burger actief is op sociale media kan hij onder meerdere grondrechten bescherming genieten. Hier wordt ingegaan op de grondrechten die in het Europees Verdrag ter bescherming van de Rechten van de Mens en de Fundamentele Vrijheden (EVRM) zijn opgenomen. In dit kader komt het recht op de persoonlijke levenssfeer (artikel 8 EVRM) het meest prominent in beeld, maar ook de grondrechten van de vrijheid van godsdienst (artikel 9 EVRM), van meningsuiting (artikel 10 EVRM) en van vereniging (artikel 11 EVRM) kunnen in verband worden gebracht met sociale media. Omdat de voorwaarden waaronder inbreuken op deze grondrechten zijn toegestaan dezelfde systematiek volgen, wordt hier verder volstaan met het behandelen van het recht op de persoonlijke levenssfeer.

Wanneer de AIVD bij zijn taakuitvoering een inbreuk maakt op het recht op de persoonlijke levenssfeer, geldt dat die inbreuk in elk geval moet voldoen aan de eisen die uit artikel 8 van het EVRM voortvloeien. Dit betekent dat de inbreuk in overeenstemming met de wet moet zijn en noodzakelijk in een democratische samenleving. De inbreuk moet zijn vereist op grond van één van de in artikel 8 genoemde belangen, waaronder het belang van de nationale veiligheid. De wettelijke regeling dient voldoende nauwkeurig geformuleerd te zijn, opdat de burger in staat is zijn gedrag daarop af te stemmen en tevens in staat is redelijkerwijs te voorzien welke gevolgen uit een bepaalde handelwijze kunnen voortvloeien. Tevens zal de inbreuk moeten voldoen aan de eisen van proportionaliteit en subsidiariteit.

Een groot deel van de informatie die via sociale media kan worden vergaard, betreft niet-afgeschermde informatie in het publieke domein, soms nadrukkelijk door betrokkenen voor een breed publiek gepubliceerd.[8] Hierbij valt te denken aan openbare profielen, online toespraken of foto's die op een vrij toegankelijke website worden geplaatst. Deze informatie kan zonder gebruik van bijzondere methodes direct door medewerkers van de AIVD of via agenten van de dienst worden verzameld.

De vraag kan worden gesteld wanneer bij de verzameling van deze openlijk beschikbare gegevens sprake is van een inbreuk op de privacy. De jurisprudentie van het Europees Hof voor de Rechten van de Mens (EHRM) en de toenmalige Europese Commissie voor de Rechten van Mens (ECRM) biedt aanknopingspunten ten aanzien van de reikwijdte van de bescherming van de persoonlijke levenssfeer in de publieke ruimte. Vooral de jurisprudentie die ziet op het monitoren van personen in het publieke domein, ontwikkeld in het kader van cameratoezicht en publieke demonstraties, bevat relevante afwegingen voor de vraag of er sprake is van een inbreuk op het recht op de persoonlijke levenssfeer.

Een voorbeeld dat zich goed laat toepassen in de context van sociale media is een uitspraak van de ECRM over het nemen van foto's door de politie bij openbare demonstraties. De ECRM gaat hierbij in op de reikwijdte van het begrip persoonlijke levenssfeer.

> "In the present case, the Commission has noted the following elements: first, there was no intrusion into the "inner circle" of the applicant's private life in the sense that the authorities entered his home and took the photographs there; secondly, the photographs related to a public incident, namely a manifestation of several persons in a public space, in which the

[8] Deze informatie kan dan ook worden getypeerd als 'open source intelligence' (osint). Onder osint wordt door de AIVD ook informatie gerekend die beschikbaar is bij commerciële bedrijven en die slechts na betaling toegankelijk is.

> applicant was voluntarily taking part; and thirdly, they were solely taken for the purposes, on 17 February 1988, of recording the character of the manifestation and the actual situation at the place in question, e.g. the sanitary conditions, and, on 19 February 1988, of recording the conduct of the participants in the manifestation in view of ensuing investigation proceedings for offences against the Road Traffic Regulations."[9]

Verder achtte de ECRM van belang dat geen namen bij de foto's werden genoteerd, de foto's verder niet werden verwerkt, en niet werd getracht om de personen te identificeren. De ECRM stelde zich om de voorgaande redenen op het standpunt dat de genomen foto´s niet binnen de reikwijdte van het begrip persoonlijke levenssfeer vielen en dat daarop dus geen inbreuk was gemaakt.
In het kader van cameratoezicht heeft het EHRM deze jurisprudentie verder ontwikkeld:

> "Article 8 also protects a right to identity and personal development, and the right to establish and develop relationships with other human beings and the outside world […]. There is also a zone of interaction of a person with others, even in a public context, which may fall within the scope of "private life".
>
> There are a number of elements relevant to a consideration of whether a person's private life is concerned by measures effected outside a person's home or private premises. Since there are occasions when people knowingly or intentionally involve themselves in activities which are or may be recorded or reported in a public manner, a person's reasonable expectations as to privacy may be a significant, although not necessarily conclusive, factor. A person who walks on the street will, inevitably, be visible to any member of the public who is also present. Monitoring by technological means of the same public scene (for example, a security guard viewing through closed-circuit television) is of a similar nature. Private-life considerations may arise, however, once any systematic or permanent record comes into existence of such material from the public domain. It is for this reason that files gathered by the security services on a particular individual fall within the scope of Article 8, even where the information has not been gathered by any intrusive or covert method."[10]

In een latere uitspraak herhaalde het Hof zijn oordeel in andere woorden:

> "The monitoring of the actions of an individual in a public place by the use of photographic equipment which does not record the visual data does not, as such, give rise to an interference with the individual's private life. […] On the other hand, the recording of the data and the systematic or permanent nature of the record may give rise to such considerations. Accordingly, in both Rotaru and Amann […] the compilation of data by security services on particular individuals, even without the use of covert surveillance methods, constituted an interference with the applicants' private lives."[11]

Of sprake is van een inbreuk hangt dus ten dele af van de gerechtvaardigde verwachtingen van de individu omtrent zijn privacy. Het enkele kennisnemen van informatie in het publieke domein door de overheid over een concreet individu leidt niet zonder meer tot een inbreuk op het privéleven van die persoon.[12] Wel acht het Hof een inbreuk al snel aanwezig indien vervolgens de persoonsgegevens (al dan niet systematisch) worden bewaard. Ook

---

[9] Europese Commissie voor de Rechten van de Mens, 19 mei 1994, *Friedl t. Oostenrijk*, 15225/89, r.o. 49. In dezelfde lijn oordeelde het ECRM in: *Herbecq e.a. t. België* , 14 januari 1998, 32200/96, r.o. 3.
[10] EHRM, 25 september 2001, *P.G. en J.H. t. het Verenigd Koninkrijk*, 44787/98, r.o. 56-57.
[11] EHRM, 28 januari 2003, *Peck t. het Verenigd Koninkrijk,* 44647/98, r.o. 59.
[12] Het Hof had weinig woorden nodig om het gericht monitoren van het gehele internetverkeer van een specifiek persoon aan te merken als een inbreuk op het recht op privacy. EHRM, 3 april 2007, *Copland t. het Verenigd Koninkrijk*, 62617/00, r.o. 43.

indien gericht over een specifiek persoon gegevens worden verzameld door veiligheidsdiensten moet dit als een inbreuk worden aangemerkt. Verder is het gebruik van heimelijke of verdekte methoden een omstandigheid waarin sneller van een inbreuk sprake zal zijn. Het enkele feit dat gebruik wordt gemaakt van technische middelen – inherent verbonden aan internetonderzoek – maakt echter nog niet dat er sprake is van een inbreuk.

Het Hof heeft zich tot op heden nog niet rechtstreeks uitgelaten over de toepassing van de rechten uit het EVRM op de sociale media. Op basis van de aangehaalde jurisprudentie komt de Commissie echter tot de volgende uitgangspunten.

Bij het vaststellen in hoeverre een inbreuk op het recht op privacy wordt gemaakt bij het verzamelen van inlichtingen uit het publieke domein, gaat het om de intentie, methoden en het product van het inlichtingenwerk. Er is sneller sprake van een inbreuk als bij het verzamelen wordt *beoogd* informatie over een concreet individu te verzamelen, gebruik wordt gemaakt van bijzonder indringende of heimelijke *methoden*, of daadwerkelijk gericht informatie over een specifiek individu wordt *opgeslagen*. Daarentegen kan worden aangenomen dat wanneer zonder heimelijke methodes informatie uit open bronnen wordt geanalyseerd, zonder dat daarbij gericht naar een bepaald individu wordt gekeken, er niet snel sprake zal zijn van een inbreuk op de persoonlijke levenssfeer van betrokkenen. Naarmate gerichter of met gebruikmaking van indringender methoden wordt gekeken naar een persoon, of hierbij persoonsgegevens worden opgeslagen, zal al snel sprake zijn van een inbreuk op de persoonlijke levenssfeer. Hiervoor zal dan een afdoende wettelijke grondslag en rechtvaardiging noodzakelijk zijn.

4.2 Wiv 2002

Naast de algemene bevoegdheid tot het verzamelen van gegevens geeft de wet een uitputtende opsomming van bijzondere bevoegdheden waarover de AIVD beschikt. In het kader van dit diepteonderzoek naar het operationeel gebruik van sociale media zijn met name de bevoegdheden tot observeren (artikel 20), de inzet van agenten (artikel 21) en het binnendringen in een geautomatiseerd werk, het zogenaamde hacken (artikel 24), van belang.

Bijzondere bevoegdheden kunnen door de AIVD slechts worden toegepast indien dit noodzakelijk is voor onderzoek ten behoeve van de veiligheidstaak of de inlichtingentaak buitenland (artikel 18 jo. artikel 6). Er dient toestemming door het hiertoe bevoegd gezag te worden verleend (artikel 19) en de inzet dient te voldoen aan de beginselen van proportionaliteit en subsidiariteit (artikelen 31 en 32). Bovendien dient een schriftelijk verslag te worden opgemaakt van de uitoefening van een bijzondere bevoegdheid (artikel 33). Voor verschillende bijzondere bevoegdheden vereist de wet dat in het verzoek om toestemming voor de inzet daarvan de reden wordt vastgelegd waarom de toepassing van het middel noodzakelijk is. De Commissie is van oordeel dat uit de wet voortvloeit dat ook voor de inzet van agenten en het hacken de motivering dient te worden vastgelegd. Dit maakt de uitoefening van deze bevoegdheden transparant en toetsbaar voor interne verantwoording en extern toezicht. Het interne beleid van de AIVD is daar overigens in lijn mee en vereist dat ook bij deze bijzondere bevoegdheden de aanvraag voor toestemming van een motivering wordt voorzien.

Opgemerkt dient te worden dat in de parlementaire behandeling van de Wiv 2002 het verzamelen van gegevens op sociale media niet afzonderlijk is benoemd. Internet komt in de

parlementaire geschiedenis slechts ter sprake waar het de bijzondere bevoegdheden op het vlak van interceptie en hacken betreft.[13]

4.2.1 Algemene bevoegdheid

Het verwerven van inlichtingen uit sociale media is een vorm van gegevensverwerking in de zin van artikel 1, sub f, van de Wiv 2002. In artikel 12 is de algemene bevoegdheid van de AIVD neergelegd om gegevens te verwerken. Het gaat hier om zowel de verwerking van persoonsgegevens als van andere gegevens. De verwerking van gegevens vindt slechts plaats voor een bepaald doel en voor zover dat noodzakelijk is voor een goede taakuitvoering (tweede lid). De verwerking van gegevens dient verder op een behoorlijke en zorgvuldige wijze plaats te vinden (derde lid). Wanneer het de verwerking van persoonsgegevens betreft kan dit bovendien slechts betrekking hebben op de in artikel 13 geduide personen.[14] De verwerking van gegevens van andere personen, hier verder aangeduid als overige gebruikers, mag slechts plaatsvinden indien dit noodzakelijk is voor de goede taakuitvoering of ter ondersteuning daarvan.

Artikel 17 geeft de AIVD de bevoegdheid om bij de uitvoering van zijn taak, of ter ondersteuning daarvan, zich te wenden tot bestuursorganen, personen en instellingen die gegevens verwerken (informanten). Hieronder kunnen ook bedrijven worden begrepen die gegevens in verband met sociale media verwerken. Zo kan de AIVD een dergelijk bedrijf vragen vanaf welk IP-adres is ingelogd door een bepaalde gebruiker. Het aangezochte bedrijf is niet verplicht om de informatie te verstrekken; de verstrekking geschiedt vrijwillig. De AIVD mag enkel om informatie vragen voor zover dat noodzakelijk is voor een bepaald doel en ter vervulling van de wettelijke taken. Daarenboven is de Commissie in het algemeen van oordeel dat de AIVD slechts gebruik kan maken van een informant voor zover het tot de normale werkzaamheden van de informant behoort om kennis te nemen van de gevraagde gegevens of deze aan derden te verstrekken. Indien het de normale hoedanigheid van de menselijke bron te buiten gaat, dan dient deze als agent te worden aangemerkt.

De algemene bevoegdheid van artikel 17 biedt naar het oordeel van de Commissie onvoldoende grondslag om een verdergaande inbreuk te maken op de persoonlijke levenssfeer, zoals bij het verwerven van de inhoud van niet-openbare communicatie bijvoorbeeld van afgeschermde berichten op sociale media. In dat laatste geval wordt een dermate verregaande inbreuk gemaakt op de persoonlijke levenssfeer dat dit slechts geoorloofd is indien daarbij aanvullende waarborgen van toepassing zijn. Het gaat hierbij onder meer om vereisten aan het toestemmingsniveau, de motivering, de verslaglegging en het gebruik van de verworven gegevens. In de wet zijn die waarborgen verbonden met de toepassing van bijzondere bevoegdheden. Nu dergelijke wettelijke waarborgen bij artikel 17 ontbreken, is die bevoegdheid niet toereikend voor het verwerven van de inhoud van afgeschermde berichten.

Ten overvloede merkt de Commissie nog op dat dit oordeel slechts de inzet van een menselijke bron voor de verwerving van de inhoud van niet openbare communicatie

---

[13] Ten aanzien van hacken: *Kamerstukken II*, 1999/2000, 25 877, nr. 8 (NV), p. 64, en ten aanzien van het tappen van elektronisch berichtenverkeer: *Kamerstukken II*, 1997/98, 25 877, nr. 3 (MvT), p. 41.

[14] Hierna wordt gesproken van 'targets' waar het de personen betreft die genoemd worden in artikel 13, eerste lid, onder a en c. Tevens worden daaronder in dit toezichtsrapport gerekend de groepen en organisaties waartoe deze personen behoren.

aangaat. Deze gegevens komt een hoger beschermingsniveau toe dan, bijvoorbeeld, financiële data die goed op grond van artikel 17 kunnen worden verworven.[15]

Het derde lid van het artikel verklaart eventuele andere wettelijke voorschriften die gelden voor de verstrekking van deze gegevens buiten toepassing indien op grond van dit artikel informatie aan de AIVD wordt verstrekt. Vaak zal het verstrekken van persoonsgegevens aan derden bijvoorbeeld niet zijn toegestaan vanwege privacywetgeving. Op grond van het derde lid mag een bedrijf deze dan toch aan de AIVD verstrekken.

4.2.2 Observatie

Een bijzondere bevoegdheid die relevant kan zijn in relatie tot sociale media, is de bevoegdheid tot observatie op grond van artikel 20, eerste lid, van de Wiv 2002. Het betreft hier de bevoegdheid tot het observeren en volgen van een natuurlijke persoon en in het kader daarvan het vastleggen van gedragingen van die persoon. De vraag is wanneer de activiteiten van de AIVD op sociale media als observatie in de zin van de wet moeten worden aangemerkt. Evenmin als bij de hiervoor besproken bijzondere bevoegdheid tot de inzet van agenten, is bij de behandeling door het Parlement van de Wiv 2002 indertijd aandacht besteed aan de toepassing van deze bevoegdheid in de omgeving van het internet.

Reeds eerder heeft de Commissie zich in algemene termen uitgesproken over de interpretatie van de bevoegdheid tot observatie:

> "Wat er onder het begrip observatie moet worden verstaan, wordt in de wetsgeschiedenis van de WIV 2002 niet nader toegelicht. […] De Commissie overweegt dat daarbij niet het doel maar de indringendheid van de observatie doorslaggevend is. Bij de vraag wanneer er sprake is van stelselmatige observatie kan tevens aansluiting worden gezocht bij de in het strafrecht geformuleerde criteria, te weten: de duur van de observatie, de plaats, de intensiteit, de frequentie of het toepassen van een technisch hulpmiddel dat meer biedt dan alleen versterking van de zintuigen."[16]

Naar het oordeel van de Commissie is sprake van observatie op sociale media door de AIVD, waarvoor een toestemming op grond van artikel 20 Wiv 2002 vereist is, indien door bijvoorbeeld de duur of intensiteit van het waarnemen een min of meer volledig beeld van bepaalde aspecten van iemands leven wordt verkregen. In het kader van sociale media kan hierbij worden gedacht aan het stelselmatig bijhouden van de niet-afgeschermde berichten op sociale media van een specifiek persoon.[17]

---

[15] Zie bijvoorbeeld: Toezichtsrapport van de CTIVD nr. 20 inzake financieel-economische onderzoeken door de AIVD, *Kamerstukken II* 2009/10, 29 924, nr. 50 (bijlage), paragraaf 3.3.1.

[16] Toezichtsrapport van de CTIVD nr. 4 inzake de rechtmatigheid van het AIVD-onderzoek naar de ontwikkelingen binnen de Molukse gemeenschap in Nederland, *Jaarverslag 2004/05*, paragraaf 2.2.2.

[17] Vergelijk: Memorie van toelichting bij het wetsvoorstel waarbij artikel 126g Sv is ingevoerd (*Kamerstukken II*, 1996/97, 25 403, nr. 3, p. 26-27):

> "Bij het op stelselmatige wijze waarnemen van personen gaat het, zoals gezegd om die vormen van observatie die tot resultaat kunnen hebben dat een min of meer volledig beeld wordt verkregen van bepaalde aspecten van iemands leven, bijvoorbeeld zijn contacten met een crimineel. Voor het antwoord op de vraag of sprake is van een dergelijke vorm van observatie is een aantal elementen van belang: de duur, de plaats, de intensiteit of frequentie en het al dan niet toepassen van een technisch hulpmiddel dat méér biedt dan alleen versterking van de zintuigen. Ieder voor zich, maar met name in combinatie, zijn deze elementen bepalend voor de vraag of een min of meer volledig beeld van bepaalde aspecten van iemands leven wordt verkregen."

Mandaat
Het Mandaatbesluit bijzondere bevoegdheden 2009 (hierna: het Mandaatbesluit) geeft in artikel 3, eerste lid, mandaat aan de directeur, het unithoofd en het teamhoofd om toestemming te verlenen voor een observatie. Het tweede lid vereist dat toestemming aan de minister wordt gevraagd indien bij het observeren met een technisch hulpmiddel kennis wordt genomen van 'elke vorm van gesprek, telecommunicatie, of gegevensoverdracht door middel van een geautomatiseerd werk'. De toelichting op dit artikel verduidelijkt dat in die gevallen het observeren niet verschilt met tappen, voor welke bevoegdheid uitsluitend de minister toestemming kan verlenen ingevolge artikel 25 Wiv 2002.

Voorts is in het Mandaatbesluit een uitzonderingsregel neergelegd voor de situatie waarin "overwegingen van principiële aard een rol spelen of indien zich bijzondere omstandigheden voordoen". Artikel 14, eerste lid, schrijft voor dat in die gevallen het ondermandaat buiten toepassing blijft, of dat de bevoegdheid op een hoger niveau wordt uitgeoefend. De toelichting op het Mandaatbesluit noemt als voorbeeld van een dergelijke bijzondere omstandigheid de situatie waarin de uitoefening van de bevoegdheid een groot publiek risico met zich brengt. De gemandateerde dient zelf een inschatting te maken of hiervan sprake is.

4.2.3 Inzet van agenten

Bij het onderzoek op sociale media komt in de eerste plaats de bevoegdheid van de inzet van een natuurlijk persoon op grond van artikel 21 Wiv 2002 in beeld. Hierbij gaat het om een natuurlijk persoon die in opdracht en onder supervisie van de AIVD op het internet informatie verzamelt. Dit kan ook een eigen medewerker van de AIVD betreffen die onder een aangenomen identiteit actief is op het internet.

In eerdere toezichtsrapporten heeft de Commissie reeds uitgebreid het wettelijk kader beschreven voor de inzet van agenten.[18] In het bijzonder kan hier worden gewezen op het toezichtsrapport inzake enkele langlopende agentenoperaties. De waarborgen en voorwaarden die voor elke agentenoperatie gelden, zijn ook van toepassing indien een agent op sociale media opereert. Zo dient bijvoorbeeld altijd een toestemming voor de inzet van de agent te worden gegeven door een directeur of unithoofd, die elke drie maanden door een teamhoofd dient te worden verlengd. De aanvragen dienen van een motivering te zijn voorzien waarin wordt afgewogen of de inzet van de agent voldoet aan de beginselen van noodzakelijkheid, proportionaliteit en subsidiariteit. Bij de inzet van agenten op sociale media krijgen de volgende aspecten van het wettelijk kader een bijzondere betekenis.

Uit de wetstekst noch de wetsgeschiedenis volgt duidelijk wanneer de inzet van een medewerker van de AIVD als de inzet van een agent in de zin van de wet moet worden aangemerkt. Evident is dat een medewerker van de AIVD in het publieke domein informatie kan verzamelen door, bijvoorbeeld, openbare demonstraties of bijeenkomsten te bezoeken. Dit kan eveneens op de sociale media. Een medewerker kan op het open gedeelte van het internet bijvoorbeeld een toespraak volgen of een webforum bezoeken. Evenals in het publieke domein van de straat zal de medewerker op sociale media niet onmiddellijk als

[18] Onder meer: toezichtsrapport van de CTIVD nr. 8b inzake de inzet door de AIVD van informanten en agenten, meer in het bijzonder in het buitenland. Jaarverslag 2006/07, p. 72. En: toezichtsrapport van de CTIVD nr. 37 inzake enkele langlopende agentenoperaties door de AIVD, *Kamerstukken II* 2013/14, 29 924, nr. 108 (bijlage).

zodanig herkenbaar willen zijn en dus een alias gebruiken. Ook veel doorsnee internetgebruikers zijn niet onder hun werkelijke naam op sociale media actief.[19]

De vraag is wanneer het gebruik van een dergelijke alias door een medewerker van de AIVD moet worden beschouwd als de inzet van een agent, die op grond van artikel 21 onder dekmantel opereert. Hiervan lijkt pas sprake te zijn wanneer daadwerkelijk een gefingeerde identiteit of hoedanigheid wordt geconstrueerd, hetgeen verder gaat dan het enkele gebruik van een alias. Indien het bij aanvang de bedoeling is om een virtuele identiteit op te bouwen, dan is ook het aanmaken van de enkele *nickname* al onderdeel van het gebruik van de dekmantel. Daarnaast is sprake van het opereren onder dekmantel wanneer aan een gesprek wordt deelgenomen met gebruikmaking van een gefingeerde identiteit.[20]

Een ander aspect van de deelname aan sociale media door medewerkers en agenten van de AIVD betreft het instigatieverbod, vastgelegd in artikel 21 van de Wiv 2002. Het is een agent verboden om een persoon te brengen tot ander handelen betreffende het beramen of plegen van strafbare feiten, dan waarop diens opzet reeds tevoren was gericht.

In het kader van de inzet van agenten op sociale media kan het voorkomen dat agenten actief de target-omgeving benaderen. Bij de beoordeling van deze operaties zal in het bijzonder aandacht moeten worden besteed aan het instigatieverbod en de jurisprudentie van het EHRM rondom de *agent-provocateur*, ontwikkeld in het kader van artikel 6 van het EVRM. In die jurisprudentie wordt telkens het belang benadrukt van heldere grenzen en waarborgen, alsmede van toezicht op undercover operaties.[21] Hierbij kent het EHRM wel gewicht toe aan de omgeving waarin de agent opereert. Indien er sterke aanwijzingen zijn dat een digitaal netwerk voor strafbare gedragingen wordt gebruikt, zal een agent meer vrijheid hebben om de gebruikers van dat netwerk daarover te benaderen.[22]

Hoewel de agenten van de AIVD niet werken ten behoeve van de opsporing en hun waarnemingen slechts in uitzonderlijke situaties een rol krijgen in een strafzaak, bijvoorbeeld via een ambtsbericht aan het Openbaar Ministerie, dient uitlokking te worden voorkomen. Het uitgangspunt blijft immers dat de overheid niet zelfstandig strafbare feiten mag genereren.[23] Bovendien zal, juist in de internationale context van sociale media, het optreden van een agent van de AIVD niet altijd bekend worden bij of getoetst worden door de rechter in een concrete strafzaak. Dit maakt dat hoge eisen moeten worden gesteld aan de transparantie en toetsbaarheid van de inzet van agenten.

---

[19] Hiermee wordt bedoeld dat iemand niet zijn of haar werkelijke naam gebruikt, bijvoorbeeld bij het creëren van een e-mailadres, profielpagina of gebruikersnaam. Zodoende ontstaan online identiteiten die een zekere mate van anonimiteit bieden aan internetgebruikers.

[20] In het kader van opsporing wordt het actief deelnemen aan communicatie als onderscheidend criterium aangelegd om de stelselmatige informatie-inwinning (artikel 126j Sv) af te bakenen van wat de politie vermag op grondslag van haar algemene taakstelling (artikel 3 Politiewet 2012): *Kamerstukken II* 1998/99, 26 671, nr. 3, p. 36. Ook in de literatuur wordt een zodanig onderscheid tussen actief deelnemen en het passief volgen toegepast op het verzamelen van inlichtingen op sociale media: I. Cameron, 'Foreseeability and safeguards in the area of security: some comments on ECHR case law', in: Vast Comité I, *Inzicht in toezicht*, Antwerpen: Intersentia 2013, p. 167.

[21] Onder meer: EHRM, 5 februari 2008, *Ramanauskas t. Litouwen,* 74420/01, r.o. 53-55; *Bannikova t. Rusland*, 4 november 2010, nr. 18757/06, r.o. 34-50.

[22] EHRM, 7 september 2004, *Eurofinacom t. Frankrijk*, 58753/00, p. 14-15 (Engelse vertaling).

[23] Toezichtsrapport van de CTIVD nr. 7 betreffende de uitvoering door de AIVD van een contra-terrorisme operatie, *Kamerstukken II* 2005/06, 29 944, nr. 10 (bijlage), paragraaf 4.3.

Tot slot kan de agent die op het internet wordt ingezet ook worden geïnstrueerd om maatregelen te treffen (artikel 21, eerste lid, onder a, sub 2). Zo kan de agent doelbewust 'desinformatie' verspreiden of het handelen van targets frustreren. Deze maatregelen laten zich in beginsel ook goed toepassen in een online context. De wetgever heeft overwogen dat de agent hiervoor pas mag worden ingezet indien de maatregelen niet via een andere weg (bijvoorbeeld door bestuurlijke maatregelen) kunnen worden bereikt.[24] Indien de agent ten behoeve van deze maatregelen een hack uitvoert, dan dient daarvoor bovendien afzonderlijk toestemming te worden gegeven.

Mandaat
Het Mandaatbesluit geeft in artikel 4, eerste lid, mandaat aan de directeur en het unithoofd toestemming te verlenen voor de inzet van een agent. De daaropvolgende verlengingen van deze toestemming kunnen ook door een teamhoofd worden gegeven. Het tweede lid geeft een afwijkende regeling voor de gevallen waarin de in te zetten persoon behoort tot een bijzondere categorie, zoals een arts of journalist. In die gevallen ligt het toestemmingsniveau hoger, in overeenstemming met de positie van betrokkene.

Voorts is de eerder genoemde uitzonderingsregel van toepassing in geval van overwegingen van principiële aard of bijzondere omstandigheden. Wanneer er zulke overwegingen of omstandigheden aan de orde zijn, moet van een hoger beslissingsniveau toestemming worden verkregen.

4.2.4 Hacken

Artikel 24 van de Wiv 2002 voorziet de AIVD van de bevoegdheid om, kort gezegd, te hacken en bijvoorbeeld de opgeslagen of verwerkte gegevens over te nemen.[25] De dienst mag een apparaat hacken wanneer het dit onder zich heeft, maar ook op afstand, bijvoorbeeld via het internet. De AIVD kan trachten door middel van een hack toegang te verkrijgen tot het apparaat waarmee een persoon gebruik maakt van sociale media. Daarnaast bewaart in veel gevallen de aanbieder van sociale media gebruikersgegevens of de inhoud van communicatie in een gegevensverzameling. De AIVD kan trachten door een hack toegang te krijgen tot die gegevensverzameling. In de wetsgeschiedenis is verduidelijkt dat de AIVD niet alleen een *stand-alone* computer mag hacken maar ook een netwerk van computers.[26] De Commissie is van oordeel dat ook het binnendringen op een server moet worden begrepen onder de hackbevoegdheid.

Mandaat
Het Mandaatbesluit geeft, voor zover hier relevant, mandaat aan de directeur en het unithoofd voor het hacken. Waar dit op afstand plaatsvindt is slechts de directeur gemandateerd (artikel 7, tweede lid). Net als bij de bevoegdheid tot observeren, is de toestemming voor de hack voorbehouden aan de minister indien de hack sterk lijkt op een tap (artikel 7, derde lid). Ook is de eerder genoemde uitzondering op het mandaat van

[24] *Kamerstukken II* 1999/2000, 25 877, nr. 8, p. 61 (NV).
[25] Voor de omschrijving van de bevoegdheid ex. artikel 24 Wiv 2002 heeft de wetgever nauw aansluiting gezocht bij de in artikel 138ab van het Wetboek van Strafrecht gehanteerde formulering. *Kamerstukken II* 1997/98, 25 877, nr. 3, p. 39 (MvT). De definitie van een geautomatiseerd werk wordt dan ook overeenkomstig diezelfde wet, artikel 80sexies, uitgelegd: "een inrichting die bestemd is om langs elektronische weg gegevens op te slaan, te verwerken en over te dragen".
[26] *Kamerstukken II* 1999/2000, 25 877, nr. 8, p. 63 (NV).

toepassing in geval van overwegingen van principiële aard of bijzondere omstandigheden (artikel 14).

4.2.5 Gegevensverzamelingen

In de juridische bijlage bij het toezichtsrapport inzake gegevensverwerking van telecommunicatie is ingegaan op de eisen die de wet stelt aan het verwerken van gegevensverzamelingen.[27] Samengevat komt dit kader er op neer dat de wet geen nadere regeling geeft voor het verwerken van (grote) gegevensverzamelingen, maar dat dit op basis van de algemene bevoegdheid tot gegevensverwerking kan plaatsvinden. De dienst mag deze gegevensverzamelingen gebruiken voor analyses. Ook mag de dienst gegevensverzamelingen (mede) ten behoeve van een buitenlandse dienst verwerven. Indien deze gegevens echter niet tevens direct een bijdrage leveren aan een lopend onderzoek van de AIVD, is voor de verwerving toestemming van de minister vereist (artikel 59, vijfde lid).[28]

Gerichtheid en proportionaliteit
Gerichtheid is een begrip dat in de wet wordt gebruikt bij het regelen van de bevoegdheden tot de interceptie van communicatie[29]. In die artikelen staat gerichte interceptie tegenover ongerichte interceptie waarbij in het eerste geval de betrokkene duidelijk moet worden aangeduid in de last. Bij interceptie betekent gerichtheid dat vooraf wordt bepaald van welke persoon, organisatie, frequentie, telefoonnummer of IP-adres gegevens worden verzameld.[30] De verhouding tussen het totaal aantal gebruikers en het aantal personen naar wie de AIVD op grond van de taakstellingen onderzoek doet (targets), zegt iets over de mate van gerichtheid van de verwerving van de verzameling gegevens.

De Commissie ziet zich gesteld voor de vraag of aan het begrip gerichtheid ook een beperkende betekenis moet worden toegekend bij andere bevoegdheden dan die van interceptie. Immers kunnen ook bij de inzet van een agent of een hack 'ongerichte' gegevensverzamelingen van sociale media worden verworven, zoals een webforum. De vraag moet worden beantwoord of de wet dit toestaat.

De Commissie is op de navolgende gronden van oordeel dat het begrip gerichtheid weliswaar een belangrijke rol toekomt bij het bepalen of de inzet van een bevoegdheid proportioneel is, maar dat niet op voorhand kan worden gezegd dat alle bijzondere bevoegdheden net zo (target)gericht moeten worden ingezet als gerichte interceptie. In de eerste plaats heeft de wetgever in de mogelijkheid voorzien dat de diensten gegevens verwerken van personen die op zichzelf geen legitiem onderwerp van onderzoek zijn voor de diensten, indien dit noodzakelijk is voor de ondersteuning van de goede taakuitvoering (artikel 13, onder e). In de tweede plaats bevat de wet in artikel 17 een voldoende precieze grond voor het verwerven van grotere gegevensverzamelingen op basis van vrijwilligheid, bijvoorbeeld, bij commerciële aanbieders. Ook het kabinet en het Parlement gingen er bij de behandeling van het post-Madridwetsvoorstel uitdrukkelijk vanuit dat de diensten toen reeds bevoegd waren om gegevensverzamelingen te verwerven.[31] Tot slot kan er op worden

---

[27] Toezichtsrapport nr. 38 van de CTIVD, paragraaf IV.2 van de Juridische bijlage.
[28] 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. 50 (bijlage), paragraaf 8.2.
[29] Gerichte interceptie wordt in artikel 25 Wiv 2002 beschreven, ongerichte interceptie in artikel 27 Wiv 2002.
[30] Zie verder het toezichtsrapport nr. 38 van de CTIVD, paragrafen II.2.2 en V.2.2 van de juridische bijlage.
[31] *Kamerstukken II* 2005/2006, 30 553, nr. 3, p. 13 e.v.

gewezen dat de wet bij veel bevoegdheden vereist dat van te voren uitdrukkelijk wordt aangegeven jegens wie de bevoegdheid wordt uitgeoefend.[32] Bij de bevoegdheden van artikelen 20 (observeren), 21 (inzet van een agent) en 24 (hacken) is dit niet het geval.

Terwijl de Commissie het verwerven van een ongerichte gegevensverzameling in beginsel niet uitsluit, geldt hierbij wel een verzwaarde proportionaliteitstoets. Ten aanzien van verzamelingen gegevens van sociale media merkt de Commissie op dat deze sterk uiteenlopen qua karakter. Er zijn platforms, zoals sociale netwerksites, die door een heel breed publiek worden gebruikt. Daar tegenover staan webfora met een sterk radicaal signatuur, waarop enkel gelijkgestemden actief zijn of waarvan de oprichters doelstellingen nastreven die de aandacht van de AIVD rechtvaardigen. Naarmate het platform meer algemeen van aard is, wordt in toenemende mate inbreuk gemaakt op de persoonlijke levenssfeer van de overige gebruikers en gelden steeds strengere eisen voor verwerving en nadere verwerking. Waar de verwerving de toets van noodzakelijkheid, proportionaliteit en subsidiariteit niet kan doorstaan, dient van verwerving van die gegevensverzameling als geheel te worden afgezien.[33] In dat geval is een targetgerichte bevraging nog wel toegestaan. Deze maatstaf volgend, is het de AIVD bijvoorbeeld slechts in bijzondere omstandigheden en onder aanvullende voorwaarden toegestaan de gegevensverzameling van een algemene sociale netwerksite in het geheel te verwerven.

Bewaartermijnen en gebruik van de gegevens
De wet kent geen algemene regeling voor bewaartermijnen van gegevensverzamelingen. Alleen voor ruwe gegevens uit de ongerichte interceptie van niet-kabelgebonden communicatie schrijft de wet een bewaartermijn voor (artikel 27, negende lid, Wiv 2002). Wel regelt de wet dat de dienst gegevens dient te verwijderen zodra deze hun betekenis hebben verloren voor het doel waarvoor ze werden verzameld (artikel 43). De Commissie heeft in het toezichtsrapport inzake gegevensverwerking van telecommunicatie reeds opgemerkt dat de wet geen bewaartermijnen voorschrijft voor de ruwe, ongeëvalueerde gegevens. Zij heeft in dat rapport aan de wetgever de aanbeveling gedaan in een wettelijke regeling op dit punt te voorzien.[34]

De Commissie heeft in datzelfde toezichtsrapport verder geoordeeld dat ongeëvalueerde gegevens die met behulp van bijzondere bevoegdheden zijn verzameld slechts mogen worden gebruikt in het kader van het onderzoek waarbinnen de gegevens zijn verworven of ten behoeve van een ander lopend onderzoek dat onder de veiligheids- of inlichtingentaak valt.[35] Dit is in lijn met de wettelijke restrictie dat bijzondere bevoegdheden alleen ten behoeve van de inlichtingen- en veiligheidstaken van de dienst mogen worden ingezet. Pas wanneer de gegevens geëvalueerd zijn, dat wil zeggen dat door de AIVD relevant geacht voor enig lopend onderzoek, mogen de gegevens worden gebruikt voor de uitvoering van andere taken van de dienst. Dit betekent dat gegevensverzamelingen waarin zowel geëvalueerde gegevens als ongeëvalueerde gegevens zijn ondergebracht niet als geheel ter beschikking mogen worden gesteld voor, bijvoorbeeld, veiligheidsonderzoeken.

---

[32] Zie de artikelen 20, vierde lid (observeren in een woning), 23 (openen van post), 25 (tappen), 27 (selectie van sigint), en 28 (opvragen verkeersgegevens) van de Wiv 2002.
[33] Dit geldt ongeacht de wijze van verwerving: bij hacks, de inzet van menselijke bronnen of bij ontvangst uit het buitenland.
[34] Artikel 27, negende lid. Zie verder: toezichtsrapport nr. 38 van de CTIVD, paragraaf 6 (onder 4.1).
[35] Toezichtsrapport nr. 38 van de CTIVD, paragraaf 4.3 en 6 (onder 4.2).

5. Sociale media in het inlichtingenproces

5.1 Organisatorische inbedding

Zoals in de inleiding vermeld, constateerde de Commissie eerder dat de AIVD in 2004 nog geen goede informatiepositie op het internet had.[36] De dienst had het gebruik van internet door radicaliserende jongeren al wel opgemerkt en in het Hofstad-onderzoek waren sinds 2000 de eerste ervaringen opgedaan met het onderzoek op internet.[37]

Nadien is het onderzoek naar met name het jihadistisch internet in een stroomversnelling gekomen. In het Jaarverslag 2005 ging de dienst uitgebreid in op de rol van internet in de gewelddadige jihad, vooral ook naar aanleiding van de onderzoeken naar Mohammed B.[38] De AIVD beschouwde het internet op dat moment als "een van de voornaamste aanjagers van processen van zelfstandige radicalisering en rekrutering". In 2006 werd een specialistisch internetteam opgericht om hierop in te spelen. Het is de Commissie gebleken dat inmiddels alle operationele teams in meer of mindere mate gegevens uit de sociale media verzamelen.

In deze paragraaf worden de verschillende methoden en de praktijk beschreven die de AIVD volgt bij het doen van onderzoek op sociale media.

Voor een goed begrip is het nodig kort te schetsen welke afdelingen van de AIVD in de praktijk betrokken zijn bij het onderzoek op sociale media. In de eerste plaats zijn daar de operationele teams die onderzoeken doen op grond van de a-taak (veiligheidstaak) en de d-taak (inlichtingentaak buitenland). Op basis van concrete onderzoeksopdrachten verzamelen de operationele teams de noodzakelijke gegevens. Waar het echter gaat om operaties die een breed belang of meerdere aandachtsgebieden van de AIVD dienen, kan het zijn dat de verwerving van gegevens bij een van de ondersteunende teams is belegd. Deze ondersteunende teams, elk met een eigen taakaccent, zijn inmiddels organisatorisch ondergebracht in de Joint Sigint Cyber Unit (JSCU). Deze gezamenlijke eenheid van de AIVD en MIVD staat ten dienste van beide organisaties. In de onderzoeksperiode waar de Commissie zich op heeft gericht stonden de ondersteunende teams enkel nog ten dienste van de AIVD.

5.2 Passief onderzoek op sociale media

5.2.1 Praktijk

Sinds enige jaren verrichten geautoriseerde medewerkers van de AIVD operationeel onderzoek op het internet. Net als ieder ander kan de AIVD hierdoor zoekslagen doen op het internet, zoals het naslaan van het e-mailadres van een target op Google, het bezoeken van de website van een extremistische organisatie of het lezen van Twitterberichten van iemand die in het buitenland deelneemt aan de gewelddadige jihad. Deze vorm van onderzoek op open bronnen kan worden omschreven als passief, omdat de medewerkers hierbij niet actief contact zoeken of zich bedienen van een dekmantel. Bij deze passieve vorm van onderzoek

[36] Toezichtsrapport van de CTIVD nr. 17 inzake afwegingsprocessen van de AIVD met betrekking tot Mohammed B., *Kamerstukken II* 2007/08, 29 854, nr. 22 (bijlage), paragraaf 7.4.
[37] AIVD, *Jaarverslag* 2004, pp. 20 en 36.
[38] AIVD, *Jaarverslag* 2005, pp. 17, 25 en 27.

beperkt de dienst zich tot het verzamelen van gegevens van het internet voor zover dit als 'open bron' geldt. Het betreft dan ook een vorm van *open source intelligence* (osint).

Omdat het internet 'open' is in allerlei gradaties, rijst de vraag welke delen van het internet de AIVD als 'open bron' mag beschouwen. De Commissie gaat hier verder uit van de uitleg die de AIVD geeft aan het begrip open bron:

> "Een bron is 'open', wanneer de verspreider (het medium) de informatie publiekelijk toegankelijk heeft gemaakt. Het maakt hierbij niet uit of moet worden ingelogd of dat voor de informatie moet worden betaald. Als de verspreider het iedereen toestaat te betalen of een inlogaccount aan te maken is het dus publiekelijk toegankelijk."

Ook websites en sociale media waarvoor moet worden ingelogd kunnen volgens deze definitie dus onder het begrip 'open bron' vallen, zolang het voor iedere andere willekeurige persoon ook mogelijk is lid te worden. Omdat een medewerker, net als op straat, hierbij niet onmiddellijk herkend wil worden, mag hierbij gebruik worden gemaakt van een fictieve naam (*nickname*).

Het onderzoek op internet is in toenemende mate ingebed in de operationele onderzoeken, waarbij de dienst ernaar streeft tot een nog beter gebruik van open bronnen-informatie te komen. Naast de handmatige zoekslagen op internet bestaan er geautomatiseerde instrumenten om berichten op sociale media te analyseren.

Het bevorderen van effectief gebruik van open bronnen is ook van belang vanuit het oogpunt van rechtmatigheid. De inbreuk die op de persoonlijke levenssfeer wordt gemaakt zal bij het raadplegen van open bronnen veelal beperkt blijven. In de wet is dan ook het beginsel vastgelegd dat eerst open bronnen moeten worden geraadpleegd voordat de AIVD overgaat tot het inzetten van bijzondere bevoegdheden (artikel 31). Het artikel bepaalt dat uitoefening van bijzondere bevoegdheden slechts is toegestaan indien de gegevens niet of niet tijdig kunnen worden verkregen via een voor eenieder toegankelijke informatiebron of een bron waarvan de dienst tot kennisneming gerechtigd is. Bovendien schrijft artikel 32 voor dat de toepassing van een bijzondere bevoegdheid wordt gestaakt, indien een minder ingrijpend middel volstaat. Dit betekent dat de AIVD zich voortdurend dient af te vragen of de manier waarop de dienst gegevens tracht te verzamelen vanuit het oogpunt van de bescherming van de persoonlijke levenssfeer wel de juiste is. Vanuit het beginsel van subsidiariteit acht de Commissie het goed dat de AIVD het gebruik van open bronnen zoveel mogelijk verankert in zijn werkprocessen.

Een aanzienlijk deel van de medewerkers van de bestudeerde teams is geautoriseerd voor het verrichten van operationele zoekslagen op het internet. Ook kan hierbij worden ingelogd op bepaalde sociale media. Het is niet eenvoudig gebleken een goed beeld te krijgen van de mate waarin er gegevens van sociale media via het passieve onderzoek worden verkregen, omdat niet altijd wordt aangeduid uit welke bron of dát gegevens van het internet zijn verkregen.

5.2.2 Bevindingen

Wat hier wordt omschreven als het passieve onderzoek op sociale media, vindt plaats op grond van de algemene bevoegdheid tot het verwerken (inclusief verwerven) van gegevens voor de AIVD (artikel 12). Op basis van de gevoerde gesprekken, constateert de Commissie dat slechts beperkt gegevens op sociale media worden verzameld door de directe toegang tot

internet. Over het algemeen verzamelen de operationele teams via andere wegen gegevens van sociale media, dan daar zelf op internet naar te zoeken. De weinige aangetroffen resultaten blijven ruimschoots binnen de grenzen van de algemene bevoegdheid tot het verzamelen van gegevens en zijn zorgvuldig verwerkt. De resultaten geven geen blijk van dermate intensief of langdurig onderzoek via het internet dat aanvullende lastgeving noodzakelijk is. Ook zijn er geen aanwijzingen dat de gepleegde zoekslagen een meer dan geringe inbreuk op de persoonlijke levenssfeer maken, en daarmee raken aan de bevoegdheid tot observatie.

Omdat het een onderzoeksmethode is die nog in ontwikkeling is en zich in de nabije toekomst wellicht verdergaande technieken zullen aandienen, acht de Commissie het op zijn plaats om een aantal waarborgen nader te bespreken.

Ten eerste moet worden gewezen op de overgang van de algemene bevoegdheid tot gegevensverwerving naar de bijzondere bevoegdheid van observatie uit artikel 20 Wiv 2002. Duidelijk is dat ook bij passief onderzoek sprake kan zijn van het heel gericht in de gaten houden van een persoon op sociale media. In het licht van de jurisprudentie van het EHRM wordt in dat geval een inbreuk gemaakt op de persoonlijke levenssfeer.[39] Indien dit stelselmatig of op meer indringende wijze gebeurt, is er sprake van een meer dan geringe inbreuk. Daar komt bij dat bij internetonderzoek veel meer gegevens kunnen worden verzameld dan een individu zelf kan waarnemen, deze gegevens kunnen worden opgeslagen, en automatische gegevensvergelijking kan in beeld komen. Onder omstandigheden is dan ook sprake van observatie van een persoon (artikel 20).[40] In die gevallen, zal er een afweging van de noodzakelijkheid, proportionaliteit en subsidiariteit moeten worden gemaakt en toestemming moeten worden gevraagd. Er bestaan op dit moment geen richtlijnen binnen de dienst aan de hand waarvan kan worden vastgesteld of voor een verdergaand of langdurig internetonderzoek een toestemming tot observatie moet worden gevraagd. De Commissie beveelt aan hiervoor een heldere maatstaf vast te leggen.

Ten tweede dient de grens met de inzet van een agent op grond van artikel 21 Wiv 2002 te worden bewaakt. Het wordt medewerkers van de AIVD toegestaan om in te loggen op sociale media met een gefingeerde identiteit. De Commissie acht het toegestaan dat een medewerker van de AIVD zich van een valse naam bedient op het internet bij diens onderzoek op grond van de algemene bevoegdheid van de AIVD. Er wordt echter een grens overschreden indien de medewerker zich actief opstelt en interactie aangaat met anderen, ook als dit slechts gebeurt om niet op te vallen. In dat geval is er sprake van opereren onder dekmantel volgens artikel 21 en wordt er van een bijzondere bevoegdheid gebruik gemaakt. Alsdan gelden de waarborgen van toestemming, motivering en verslaglegging (paragraaf 4.2.3). De Commissie constateert dat het onderscheid tot de inzet van agenten in de huidige situatie voldoende gewaarborgd is.

Ten derde merkt de Commissie op dat het gebruik van internet voor operationeel onderzoek de vraag opwerpt hoe de resultaten moeten worden vastgelegd. De Commissie acht het onwenselijk en onwerkbaar om alle waarnemingen op het internet vast te leggen, maar

---

[39] Zie paragraaf 4.1.

[40] Vergelijk: B-J. Koops e.a., *Juridische scan openbrononderzoek*, Universiteit van Tilburg en TNO 2012, p. 37-38 en p. 53. Deze studie heeft gekeken naar de bescherming van privacy bij surveillance-programma's op het internet. De auteurs maken hierbij een onderscheid tussen de niet-persoonsgerichte internetsurveillance, waarbij de inbreuk op de privacy van een geringe omvang blijft, en de verdergaande inbreuk door observatie.

relevante resultaten dienen wel te worden gedocumenteerd.[41] De eis tot goede documentatie vloeit voort uit de plicht bij gegevensverwerking zorgvuldig te werk te gaan (artikel 12, derde lid) en de betrouwbaarheid of bron van gegevens te duiden (vierde lid). Het belang bij goede registratie hangt samen met het feit dat onderzoeksresultaten worden gebruikt voor de onderbouwing van lasten, inlichtingenrapportages en ambtsberichten. Wanneer resultaten onvoldoende worden gedocumenteerd zijn deze ook niet raadpleegbaar voor andere dienstmedewerkers en neemt de controleerbaarheid van de producten van de AIVD af. Bij dit alles komt nog dat het internet veranderlijk is en informatie die vandaag te vinden is, morgen verdwenen kan zijn. Ook draagt goede registratie bij aan het bewaken van de grens ten opzichte van de observatie en inzet van agenten.

De Commissie beveelt aan het bestaande beleid voor het operationeel gebruik van internet en het vastleggen van resultaten nader te formuleren. Bovengenoemde waarborgen dienen hierbij een plaats te krijgen in het beleid. Zo dient het onderzoek op internet op basis van de algemene bevoegdheid helder te worden afgebakend van de meer inbreukmakende bijzondere bevoegdheden en dient te worden voorzien in eenduidige regels voor de registratie van resultaten. Het is de Commissie overigens bekend dat de AIVD werkt aan herziening van de interne regels rondom de registratie van resultaten.

Ten aanzien van de geautomatiseerde systemen voor het verzamelen van gegevens van het internet merkt de Commissie het volgende op. Andere sectoren van de maatschappij laten zien dat de mogelijkheden op dit vlak snel toenemen. Er bestaan inmiddels verschillende instrumenten voor sociale netwerkanalyse en het monitoren van evenementen.[42] De Commissie beveelt aan bij het ontwikkelen van nieuwe onderzoeksmethoden op het vlak van sociale media, in een vroeg stadium kennis op te doen uit andere sectoren en uit de wetenschap op het vlak van (privacy-)waarborgen en deze kennis toe te passen bij het ontwikkelen van nieuwe methoden. Op deze wijze wordt bevorderd dat nieuwe systemen vanaf ingebruikname aan alle wettelijke vereisten voldoen.

5.3 Actief onderzoek door agenten op sociale media

5.3.1 Praktijk

Net als in de stoffelijke wereld kan de AIVD ook agenten inzetten in de digitale wereld om gegevens te verzamelen. Zowel eigen medewerkers van de AIVD als niet-medewerkers kunnen op grond van artikel 21 van de Wiv 2002 worden ingezet als agenten op sociale media. De agent kan onder diens eigen identiteit actief zijn of met gebruikmaking van een gefingeerde identiteit. Vrijwel alles wat in de niet-virtuele wereld aan agenten kan worden opgedragen, is ook in de virtuele wereld mogelijk. Hierbij moet worden gedacht aan het opbouwen van vriendschappen (via Facebook), het bezoeken van bijeenkomsten van een targetgroep (op een webforum) of het volgen van open publicaties (blogs). Bij sommige

---

[41] De noodzaak tot zorgvuldige verslaglegging bleek de Commissie ook in een recente klachtzaak. De AIVD kon niet meer aangeven of bepaalde gegevens waren verzameld op het open of afgeschermde gedeelte van het internet.

[42] Elders zijn reeds uitgebreid de mogelijkheden van dit soort instrumenten en de in acht te nemen waarborgen beschreven. Zie bijvoorbeeld: J. Bartlett en C. Miller, *The state of the art: a literature review of social media intelligence capabilities for counter-terrorism.* Londen: Demos, 2013, p. 15. OVSE, *OSCE Online Expert Forum Series on Terrorist Use of the Internet: Threats, Responses and Potential Future Endeavours – Final Report*. Wenen: OVSE, 2013.

agentenoperaties opereert de agent uitsluitend op het internet, bij andere operaties vormt dit slechts een gedeelte van zijn inzet.

In de bestudeerde onderzoeken worden verschillende agenten op sociale media ingezet om gegevens te verzamelen. Het gaat hierbij om operaties waarbij de doelstellingen sterk variëren. Enkele agenten worden met name ingezet om in algemene zin signalen over radicalisering of dreigingen op te vangen op specifieke sociale media. Zij voorzien het team dan van duiding van sentimenten in een bepaalde gemeenschap en volgen de (online) discussies die plaatsvinden. Hoewel deze agenten opereren onder dekmantel is de inbreuk op grondrechten van betrokken personen relatief beperkt, voor zover het sociale media betreft, omdat de agenten zich overwegend passief opstellen. Bij andere bestudeerde agentenoperaties stellen agenten zich actiever op. Een aantal van deze agenten heeft ook toestemming gekregen strafbare feiten te plegen. Deze toestemming maakt het bijvoorbeeld mogelijk dat de agent zich op sociale media op een zodanige wijze kan uiten dat hij niet uit de toon valt.

In aanvulling op het algemeen geldende kader voor agentenoperaties heeft de AIVD in 2006 een juridisch kader opgesteld voor de *eigen* medewerkers die als agent online opereren. Hierin is onder meer voorgeschreven dat de dekmantel waaronder de agent optreedt, zijn virtuele identiteit, wordt vastgelegd en wordt bijgehouden. De eigen medewerker van de AIVD opereert veelal als agent op het internet naast zijn hoofdwerkzaamheden voor het operationele team waar hij deel van uit maakt. De medewerker is zelf verantwoordelijk voor de verslaglegging van de operatie. Dit alles wijkt af van de normale situatie waarin een externe agent wordt ingezet en waarbij sturing en verslaglegging bij de begeleider van de agent is belegd, de acquisiteur.

In 2007 is verder een leidraad opgesteld waarin is beschreven hoe agentenoperaties op internet door eigen medewerkers zorgvuldig dienen te worden uitgevoerd. Onder meer is het volgen van een specifieke opleiding hierin als voorwaarde voor de inzet van de agent voorgeschreven. Ook wordt ingegaan op de wijze waarop de agent verslag dient bij te houden van zijn activiteiten en bevindingen en van de sturing die hij ontvangt. De leidraad schrijft voor dat een bewerker uit het team de agent begeleidt. Dit is anders dan bij gewone agentenoperaties, waarbij de agent altijd wordt begeleid door een acquisiteur.

Voor de inzet van *externe* personen als agent op het internet is geen specifiek beleid vastgesteld. Wel zijn er handleidingen en een cursus ontwikkeld ten behoeve van acquisiteurs die deze agenten begeleiden. Hierin worden handreikingen gedaan tot zorgvuldige, veilige, controleerbare en effectieve inzet van agentenoperaties op internet te komen. Onder meer worden verschillende wijzen van rapportage en verslaglegging aangereikt.

Agenten kunnen naast hun werkzaamheden voor de AIVD ook privé actief zijn op sociale media. Dit kan risico's met zich meebrengen. De acquisiteurs onderkennen deze risico's en geven de agenten op dit punt begeleiding. Ten aanzien van de inzet van externe agenten volgen de acquisiteurs de gebruikelijke vormen van verslaglegging. In de dossiers wordt evenwel niet altijd bijgehouden waaruit de gefingeerde identiteit van de agent bestaat, waaronder de gebruikte *nickname*.

Een recente interne evaluatie door de AIVD heeft verschillende knelpunten in kaart gebracht bij de inzet van eigen medewerkers als agenten op het internet. De begeleiding en ondersteuning blijkt niet te beantwoorden aan de behoeften van medewerkers die als agent

online opereren. Op grond van deze evaluatie werkt de AIVD aan het verbeteren van de omstandigheden voor de online opererende medewerkers, waarbij het verbeteren van de begeleiding een belangrijk onderwerp vormt. Tevens is de behoefte onderkend dat het beleidskader dient te worden geactualiseerd.

5.3.2 Bevindingen

De Commissie is van oordeel dat de operaties waarbij *externe* agenten worden ingezet, zorgvuldig en doordacht worden uitgevoerd. De sturing die de agenten ontvangen en de gegevens die de agenten verzamelen worden op afdoende wijze vastgelegd. De Commissie benadrukt dat naarmate een agent op indringender wijze wordt ingezet, dit noopt tot het gebruik van meer nauwgezette methoden van verslaglegging.

Dat er geen afzonderlijk beleid of kader is voor dit type agentenoperaties blijkt in de praktijk niet tot problemen te leiden. Het algemene beleid voor de inzet van agenten volstaat. Wel beveelt de Commissie aan meer aandacht te besteden aan het vastleggen van de al dan niet gefingeerde online identiteiten van de agenten. Uit de dossiers moet helder zijn af te leiden welke gebruikers op sociale media agenten van de AIVD zijn. Dit is van belang voor de veiligheid van de agent en de controleerbaarheid van de operatie.

Een meer diffuus beeld heeft de Commissie verkregen daar waar het de *eigen* medewerkers betreft die als agent op het internet worden ingezet. Er ligt voor deze operaties een richtinggevend beleidskader, waar in de praktijk echter onvoldoende de hand aan wordt gehouden. Er is bij de Commissie geen twijfel dat de toestemmingen voor de bestudeerde operaties op goede gronden zijn verleend en voldoen aan de vereisten van noodzakelijkheid, proportionaliteit en subsidiariteit. De Commissie constateert wel verschillende formele tekortkomingen en een groot tekortschieten in verslaglegging.

In één geval lijkt het erop dat de inzet van de agent pas maanden na aanvang van de operatie is goedgekeurd. De toestemming voor de inzet van de agent is in dat geval niet voorzien van een datum. De Commissie beoordeelt het ontbreken van de datum als een onzorgvuldigheid die ertoe leidt dat niet kan worden vastgesteld of de toestemming bij aanvang van de operatie aanwezig was.

De noodzaak van verslaglegging vindt zijn weerslag in zowel wettelijke bepalingen als intern beleid. Zo schrijft de wet voor dat instructies aan de agent worden vastgelegd (artikel 21, zesde lid). Ook dient van de inzet van de agent schriftelijk verslag te worden opgemaakt (artikel 33). De Commissie acht het hierbij noodzakelijk dat uit het dossier van een agentenoperatie zonder meer valt vast te stellen onder welke virtuele identiteit de agent opereert. Volgens de interne beleidsregels van de AIVD dient dit te worden vastgelegd in operatierapporten over de inzet van agenten. De wet stelt nadere eisen aan de instructie waarbij strafbare feiten worden opgedragen (artikel 21, vijfde lid). In de bestudeerde operaties is de toestemming tot het plegen van strafbare feiten telkens verleend onder de voorwaarde dat regelmatig operatierapporten dienden te worden opgesteld.

Alle bestudeerde operaties door eigen medewerkers schieten op het punt van verslaglegging tekort. Voor zover operatierapporten zijn opgesteld, kan hierin niet goed worden nagegaan gaan welke instructies zijn gegeven aan de agenten. Ook is slechts zeer beperkt na te gaan welke gegevens door de agenten zijn verzameld en welke uitlatingen door de agent zijn gedaan. Voorts wordt onvoldoende inzichtelijk bijgehouden in de dossiers van de agenten onder welke virtuele dekmantel zij opereren, hetgeen van belang is voor de veiligheid van

de agent en de controleerbaarheid van de operaties. Het onderzoek door de Commissie werd bemoeilijkt door deze situatie. Het is de Commissie overigens opgevallen dat deze gebreken zich met name voordoen bij de meer intensieve operaties.

De Commissie is van oordeel dat het gebrek aan verslaglegging en het vastleggen van instructies in vijf gevallen van dien aard is dat hierdoor van een onrechtmatigheid sprake is. In deze gevallen zijn over langere periodes in het geheel geen operatierapporten opgesteld of bieden de rapporten die er wel zijn volstrekt onvoldoende inzicht in aansturing, instructies en inzet. Hieraan doet niet af dat de verzamelde gegevens door deze agenten deels zijn terug te vinden in inlichtingenproducten. De Commissie beveelt aan de verslaglegging van de lopende operaties onverwijld in lijn te brengen met de binnen de dienst gebruikelijke standaarden. De uitkomsten van de in het slot van paragraaf 5.3.1 genoemde interne evaluatie door de AIVD kunnen een bijdrage leveren aan het verbeteren van de werkprocessen op dit punt. De Commissie gaat nader in op deze operaties in de geheime bijlage.

De Commissie stelt vast dat het ontbreken van de betrokkenheid van een acquisiteur of een andere vorm van begeleiding aan de geconstateerde tekortkomingen heeft bijgedragen. Zij merkt op dat in enkele gevallen waarin op een later moment een acquisiteur bij de operatie is betrokken, er duidelijk meer aandacht is gekomen voor een zorgvuldige uitvoering van de operatie. Zij wijst erop dat de AIVD reeds gedetailleerde richtlijnen heeft voor de uitvoering van dergelijke operaties, terwijl ook de eerder genoemde interne evaluatie en de interne opleiding het belang van verslaglegging reeds onderstreepten. De Commissie beveelt aan de begeleiding van de medewerkers-agenten op het internet aanzienlijk te verbeteren en bij dit traject de vraag te betrekken hoe ook de sturing en interne verantwoording van deze operaties kan worden verbeterd. In het recent uitgebrachte toezichtsrapport inzake enkele langlopende agentenoperaties is de Commissie nader ingegaan op de wenselijkheid van periodieke evaluaties bij agentenoperaties.[43]

5.3.3 Strafbare feiten in een online omgeving

Een onderwerp dat afzonderlijke aandacht behoeft is het plegen van strafbare feiten door agenten op het internet.

Onder strikte voorwaarden kan de AIVD een agent instrueren strafbare feiten te plegen. In enkele bestudeerde operaties is hiervan ook sprake geweest. Om zich in een radicale omgeving te kunnen bewegen en discussies te kunnen volgen, kan het nodig zijn dat de agent zich radicaal uit en daarbij de grenzen van de strafwet overschrijdt. Dit is in de digitale wereld niet anders dan bij het opereren in de stoffelijke wereld. Een bijzonder aspect van het opereren op sociale media is dat een strafbaar feit dat wordt gepleegd vaak niet alleen aan Nederlandse belangen raakt, maar ook aan de belangen en rechtsorde van andere landen. Er is dan ook op enkele momenten aandacht van buitenlandse opsporingsdiensten voor agenten van de AIVD geweest.

In twee gevallen is een medewerker van de AIVD meerdere maanden als agent ingezet zonder dat de benodigde toestemming voor het plegen van strafbare feiten door het hoofd van de dienst was gegeven. In de ene operatie is de toestemming tot het plegen van de strafbare feiten lange tijd niet voorgelegd aan het diensthoofd. Toen dit na een half jaar werd

[43] Toezichtsrapport nr. 37 van de CTIVD inzake enkele langlopende agentenoperaties door de AIVD, *Kamerstukken II* 2013/14, 29 924, nr. 108 (bijlage), paragrafen 4.2.2 en 6.

ontdekt heeft het diensthoofd de toestemming alsnog gegeven. Ook in de andere operatie is de toestemming niet tijdig ondertekend door het diensthoofd. Na bijna een jaar werd alsnog een (gewijzigde) toestemming gegeven door het hoofd van de dienst. De Commissie is van oordeel dat dit ernstige formele tekortkomingen betreffen. De later afgegeven toestemmingen herstellen naar het oordeel van de Commissie niet dat hier onzorgvuldig is gehandeld. Hierbij tekent zij wel aan dat er geen reden is te veronderstellen dat de toestemmingen, indien tijdig aangevraagd, zouden zijn geweigerd.

In een andere operatie beveelt de Commissie aan alsnog te bezien of een toestemming voor het plegen van strafbare feiten dient te worden aangevraagd. De agent begeeft zich met zijn uitlatingen op het internet mogelijk over de grens van wat toelaatbaar is ingevolge de strafwet. Indien de toestemming niet wordt aangevraagd en gegeven, dan dient de agent binnen de grenzen van de Nederlandse strafwet te opereren en moet daarop worden toegezien.

In de bestudeerde operaties is in de toestemmingen voor het plegen van strafbare feiten telkens een aantal waarborgen opgenomen, die tot doel hebben de feiten te beperken, transparantie te bereiken en controle mogelijk te maken. Hierbij valt op dat, op één uitzondering na, er telkens van is afgezien om de Landelijk Officier van Justitie (LOvJ) in kennis te stellen van de toestemming strafbare feiten te plegen. De Commissie wijst erop dat volgens het interne beleid de LOvJ in beginsel in kennis dient te worden gesteld van een toestemming tot het plegen van strafbare feiten. In het in juni 2014 verschenen toezichtsrapport inzake enkele langlopende agentenoperaties heeft de Commissie aanbevolen de LOvJ te informeren over *alle* toestemmingen voor het plegen van misdrijven.[44] De LOvJ kan immers advies geven bij het wegen van de proportionaliteit van de toegestane strafbare feiten, het voorkomen van strafbare feiten en het formuleren van de toegestane handelingen. In het uiterste geval kan deze een rol spelen bij het beschermen van de agent tegen eventuele strafvervolging.

In de operaties waarin géén toestemming voor het plegen van strafbare feiten is gegeven, dienen de agenten binnen de grenzen van de strafwet te blijven. Bij *externe* agenten ziet de acquisiteur daar op toe. De Commissie is van oordeel dat de acquisiteurs in de bestudeerde operaties hier voldoende invulling aan geven.

Vanwege het ontbreken van een acquisiteur bij het online opereren van *eigen* medewerkers, is het juist dan van belang dat verslaglegging zorgvuldig geschiedt. Goede verslaglegging dient de interne verantwoording en het extern toezicht door de Commissie. Bij online agentenoperaties is het bovendien goed mogelijk transparant te werken vanwege de vele mogelijkheden om (digitaal) verslag te laten opmaken door agenten. De Commissie merkt in dit verband op dat het tekortschieten in het vastleggen van instructies en de verslaglegging, zich extra laat voelen waar toestemming voor het plegen van strafbare feiten is gegeven. In een aantal toestemmingen is goede verslaglegging met zoveel woorden ook opgenomen als voorwaarde waaronder de toestemming wordt verleend. De Commissie wijst nogmaals op de jurisprudentie van het EHRM (zie paragraaf 4.2.3) en de daarin benoemde waarborgen van sturing, transparantie en controle bij de inzet van agenten.

[44] Bij spoedgevallen dient de LOvJ achteraf geïnformeerd te worden. Zie toezichtsrapport nr. 37 van de CTIVD inzake enkele langlopende agentenoperaties door de AIVD, *Kamerstukken II* 2013/14, 29 924, nr. 108 (bijlage), paragrafen 5.2.1.

In vier van de in paragraaf 5.3.2 reeds besproken agentenoperaties door eigen medewerkers is een toestemming voor het plegen van strafbare feiten gegeven. Het tekortschieten in de verslaglegging bij deze operaties betekent ook dat ten aanzien van het plegen van strafbare feiten niets is vastgelegd. Deze tekortkoming is van dien omvang dat hier sprake is van een onrechtmatigheid bij de uitvoering van de toestemming tot het plegen van strafbare feiten. Door een gebrek aan verslaglegging valt voor de Commissie niet te beoordelen of aan deze agenten voldoende sturing is gegeven dan wel voldoende is toegezien op het naleven van het verbod op uitlokking.

In het in juni 2014 verschenen toezichtsrapport inzake enkele langlopende agentenoperaties doet de Commissie aanbevelingen inzake de procedures rondom het plegen van strafbare feiten door agenten.[45] De hierboven beschreven problemen bevestigen naar het oordeel van de Commissie de noodzaak voor de AIVD op korte termijn die aanbevelingen te implementeren.

5.4 Onderzoek door het verwerven van gegevensverzamelingen van sociale media

5.4.1 Praktijk

Behalve de hiervoor beschreven manieren om op passieve of actieve wijze gegevens te verzamelen *op* sociale media, richt de dienst zich op het verwerven van gegevensverzamelingen *van* sociale media. Deze gegevensverzamelingen bevatten inhoud en/of metagegevens van communicatie op sociale media. Vanwege de vragen die leven in de samenleving, zal hierbij afzonderlijk aandacht worden besteed aan webfora.

De AIVD kan targetgerichte bevragingen uitvoeren bij aanbieders van sociale media, of trachten een (deel van hun) gegevensverzameling te verkrijgen. De wet biedt verschillende mogelijkheden hiertoe. Zo kan de dienst gebruik maken van hacks of menselijke bronnen (zowel informanten op grond van artikel 17 als agenten op grond van artikel 21). Als de menselijke bron verzamelingen gegevens zoals webfora aan de AIVD verstrekt, zal dit vaak zijn normale werkzaamheden te buiten gaan en wordt deze menselijke bron aangemerkt als een agent. Ook kan de AIVD van een buitenlandse dienst een gegevensverzameling verkrijgen of via die buitenlandse dienst gerichte bevragingen uitvoeren.

In de meeste gevallen betreft het bij deze bevragingen en verwervingen van gegevensverzamelingen 'opgeslagen' gegevens. Dit betekent dat deze gegevens niet de hogere mate van bescherming kennen, zoals de Grondwet die geeft aan 'stromende' (*real time*) gegevens. Wanneer het wel om 'stromende' gegevens gaat dient de minister toestemming te geven de communicatie te intercepteren, net als bij een tap.[46] Voor hacks is dit strengere regime vastgelegd in het Mandaatbesluit, en voor de inzet van menselijke bronnen volgt dit uit recent intern beleid van de AIVD.[47]

De gegevensverzamelingen van sociale media kunnen van belang zijn voor meerdere onderzoeken van de AIVD. Immers kan een target in een onderzoek naar extremisme bij toeval gebruik maken van hetzelfde platform van sociale media als een target in een contra-

[45] Toezichtsrapport nr. 37 van de CTIVD inzake enkele langlopende agentenoperaties door de AIVD, *Kamerstukken II* 2013/14, 29 924, nr. 108 (bijlage), paragraaf 6.
[46] Artikel 13 van de Grondwet.
[47] Zie hierover verder: toezichtsrapport nr. 38 van de CTIVD, paragraaf 6 (onder 6.3.4 en 6.3.5).

inlichtingenonderzoek. Aangezien de gegevensverzameling mogelijk uiteenlopende onderzoeken kan dienen, is het bevragen, verwerven en ontsluiten hiervan belegd bij het ondersteunende team. Dit team onderzoekt uit zichzelf en op verzoek van operationele teams de mogelijkheden om specifieke gegevens te verzamelen of gegevensverzamelingen in hun geheel te verwerven. De specifieke taak van het ondersteunende team sluit echter niet uit dat een operationeel team ook zelf een gegevensverzameling verwerft. In een beperkt aantal gevallen gebeurt dit ook.

Gerichte bevragingen van gegevensverzamelingen via menselijke bronnen worden door de acquisiteurs van het ondersteunende team uitgevoerd. Het operationele team levert in dat geval concrete vragen aan ten aanzien van personen of organisaties. De acquisiteur legt deze vragen voor aan de menselijke bron.

In het geval van webfora kan het gaan om de integrale verwerving van een webforum. Bij de verwerving van het forum wordt dan niet op voorhand enig targetgericht selectiecriterium toegepast. Alle uitgewisselde communicatie van alle gebruikers (targets en overige gebruikers) wordt gekopieerd en doorzoekbaar gemaakt. Zoals de Commissie reeds in haar toezichtrapport inzake gegevensverwerking van telecommunicatie heeft geconstateerd, wordt bij het beheer van de applicatie waarin deze gegevens zich bevinden op zorgvuldige wijze invulling gegeven aan het wettelijk vereiste dat slechts toegang wordt gegeven voor zover dat noodzakelijk is voor een goede uitvoering van de aan de desbetreffende medewerker opgedragen taak (artikel 35 Wiv 2002).[48]

In het interne beleid van de dienst voor de uitvoering van veiligheidsonderzoeken is echter opgenomen dat bij bepaalde veiligheidsonderzoeken wordt gecontroleerd of er gegevens uit webfora beschikbaar zijn over de betrokken persoon. De teams die de veiligheidsonderzoeken uitvoeren hebben zelf geen directe toegang tot deze gegevens, maar kunnen gerichte vragen stellen aan daarvoor aangewezen medewerkers van de operationele teams. Hierbij is het onder omstandigheden volgens het intern beleid van de dienst mogelijk voor veiligheidsonderzoekers kennis te nemen van de inhoud van de communicatie van een betrokkene op een webforum. Het kan hierbij niet alleen gaan om gegevens die reeds zijn betrokken in een operationeel onderzoek van de AIVD, maar ook ongeëvalueerde (ruwe) gegevens.

5.4.2 Bevindingen

a) Verwerving door middel van hacken

De door de Commissie bestudeerde hacks die door de AIVD zijn uitgevoerd om webfora te verwerven zijn in alle gevallen goed gemotiveerd. De gehackte webfora waren telkens als geheel relevant voor de taakuitvoering van de AIVD. De toestemming voor de hack is in het algemeen gegeven op het daartoe bevoegde beslisniveau. De Commissie acht het niet zorgvuldig dat in enkele gevallen door een unithoofd toestemming is gegeven voor de verlenging van een hack op afstand. Hiervan is sprake als de AIVD geen directe fysieke toegang heeft tot het te hacken geautomatiseerd werk. Volgens het interne beleid en het Mandaatbesluit is dan slechts de directeur bevoegd om toestemming te verlenen voor de inzet of de verlenging van de hack.[49]

b) Motivering van de inzet van menselijke bronnen

[48] Toezichtsrapport nr. 38 van de CTIVD, paragraaf 4.3.
[49] Overigens wordt dit beleid op dit moment herzien.

De menselijke bronnen (informanten en/of agenten) die gegevensverzamelingen verwerven of die (target)gerichte bevragingen uitvoeren, worden voornamelijk door het ondersteunende team ingezet. De aanvragen in verband met deze operaties worden dan ook door dit team opgesteld en voorzien van een motivering. Dit team gebruikt de verworven gegevens niet zelf voor enig onderzoek, het is immers het operationeel team dat dit doet. Dit maakt dat het ondersteunende team niet optimaal in staat is om de inzet en opbrengst van deze menselijke bronnen op waarde te schatten. Sinds begin 2013 wordt in het geheel geen afweging meer gemaakt van de proportionaliteit van de inzet van deze bronnen. Er zijn geen afspraken op basis waarvan de operationele teams een motivering dienen vast te leggen. Bovendien volgt uit verschillende organisatiedocumenten dat het ondersteunende team de verantwoordelijkheid draagt voor de juiste toepassing van de voorschriften bij de inzet van agenten door dit team.

De Commissie is ten aanzien van vijf *agenten*operaties van oordeel dat de motivering van de inzet van de desbetreffende agenten dermate tekortschiet dat de toestemmingen hiervoor onrechtmatig zijn gegeven. In deze vijf operaties voerden de agenten ook handelingen uit die met hacken te vergelijken zijn.[50] In de initiële aanvragen of de aanvragen tot verlenging is slechts summier aandacht besteed aan de noodzakelijkheid en de beginselen van proportionaliteit en subsidiariteit van de inzet van de agent. Er wordt volstaan met gemeenplaatsen, zonder dat wordt gemeld welke gebruikers in onderzoek zijn of welke inbreuk op de levenssfeer van overige gebruikers wordt gemaakt. Ook wordt geen aandacht besteed aan de mogelijkheden om de inbreuk op persoonlijke levenssfeer van overige gebruikers te beperken.

Dit heeft in elk geval tot gevolg gehad dat meerdere webfora zijn verworven terwijl bij aanvang geen zorgvuldige afweging van noodzakelijkheid, proportionaliteit en subsidiariteit was vastgelegd. Onder *c)* wordt nader ingegaan op de vraag of de verwerving van deze webfora voldeed aan het vereiste van proportionaliteit.

De Commissie heeft er oog voor dat in de beginfase van het werken met gegevensverzamelingen niet altijd duidelijk is geweest op welke wettelijke grondslag de dienst deze mocht verwerven, en hoe aan de verplichting tot het motiveren invulling diende te worden gegeven. Deze pioniersfase is echter reeds een aantal jaren voorbij. In maart 2013 is er een intern voorstel opgesteld om de motivering van de lasten te verbeteren. De uitvoering van dit voorstel is echter niet ter hand genomen in de onderzoeksperiode, zodat het geconstateerde gebrek in de motiveringen bleef voortbestaan. De AIVD heeft aan de Commissie medegedeeld dat de werkwijzen kort geleden zijn aangepast, hetgeen nog wel moet worden vertaald in de interne beleidsregels.[51] De Commissie is van mening dat van de dienst een alertere houding op dit punt had mogen worden verwacht.[52] De Commissie beveelt aan om op korte termijn de aangepaste werkwijzen in beleid vast te leggen.

---

[50] De Commissie benoemde deze operaties reeds in het rapport over gegevensverwerking van telecommunicatie, en komt na nader feitenonderzoek tot deze beoordeling. Toezichtsrapport nr. 38 van de CTIVD, paragraaf 3.4.2.

[51] De AIVD heeft in zijn reactie op het opgestelde rapport aangegeven dat inmiddels de nieuwe werkwijze wordt toegepast. Volgens deze nieuwe werkwijze dragen de operationele teams die de inzet van de bevoegdheid wenst, zorg voor de motivering.

[52] Reeds eerder heeft de Commissie de aanbeveling gedaan ook bij het verkrijgen van webfora van een buitenlandse dienst de overweging vast te leggen in hoeverre het kennis nemen van de inhoud van het desbetreffende webforum voldoet aan het noodzakelijkheids-, proportionaliteits- en subsidiariteitsvereiste. Toezichtsrapport nr. 38 van de CTIVD, paragraaf 3.5.5.

c) Proportionaliteit en gerichtheid

De mate van de inbreuk op de persoonlijke levenssfeer bij het verwerven van gegevensverzamelingen loopt sterk uiteen. In bepaalde gevallen is deze inbreuk zeer gering. Zo valt het verwerven van bepaalde gebruikersgegevens in sommige gevallen nog het best te vergelijken met de aanschaf van een telefoonboek, waardoor gebruikers aan IP-adressen kunnen worden gekoppeld. Commerciële aanbieders hebben dergelijke gegevensverzamelingen soms al kant en klaar liggen en ontsluiten deze informatie voor marketingdoeleinden. In andere gevallen wordt bijvoorbeeld (het besloten deel van) een webforum met de inhoud van berichten van alle gebruikers verkregen, hetgeen een verregaande inbreuk op de persoonlijke levenssfeer van betrokkenen betekent. Naarmate de inbreuk verdergaand is, gelden steeds strengere voorwaarden voor verwerving en strengere waarborgen die bij de verwerking in acht dienen te worden genomen (zie hierover verder paragraaf 4.2.5). Dit geldt nog meer indien daarbij ook een inbreuk wordt gemaakt op de persoonlijke levenssfeer van overige gebruikers die niet relevant zijn voor enig operationeel onderzoek van de dienst.

De Commissie constateert dat de afdeling juridische zaken van de AIVD in 2011 een gedegen beleidsnotitie over het verwerven van gegevensverzamelingen heeft opgesteld, waarin alle relevante waarborgen een plaats hebben. De implementatie hiervan is echter niet ter hand genomen. Het gebrek aan uitvoering van het beleid laat zich voelen in de praktijk. Zoals de Commissie hierna beschrijft, is er een viertal gegevensverzamelingen waarvan de Commissie de verwerving onrechtmatig acht. De Commissie beveelt aan dat op korte termijn bindend beleid wordt vastgesteld op het punt van de verwerving van gegevensverzamelingen (waaronder webfora).

De webfora die door de AIVD in de onderzoeksperiode zijn verworven zijn bestudeerd door de Commissie. De Commissie stelt vast dat het in vrijwel alle gevallen webfora betreft waarvan de verwerving noodzakelijk was voor de taakuitvoering van de dienst. Deze webfora hebben een overwegend radicaal of extremistisch signatuur, of de personen of organisaties die het beheer voeren over de webfora zijn een gevaar voor nationale veiligheid of democratische rechtsorde. De virtuele groep van gebruikers en beheerders van het webforum kan in die gevallen als een targetorganisatie worden aangemerkt, die – net als in de tastbare wereld – een legitiem onderwerp van onderzoek kan zijn.

De Commissie constateert dat bij enkele webfora een dergelijk radicaal of extremistisch signatuur van het forum of van de beheerders ontbreekt. In die gevallen kan het webforum niet als zodanig, in zijn geheel, worden aangemerkt als legitiem onderwerp van onderzoek. Voor het verwerven van een dergelijk webforum geldt een verzwaarde proportionaliteitstoets. Hierbij weegt zwaar dat er gegevens in de verzameling zitten van (vele) overige gebruikers die niet relevant zijn voor de AIVD.[53] Indien het operationele belang bij de verwerving zo zwaar weegt dat het toch proportioneel is om de gehele gegevensverzameling te verwerven, dan dient nog immer de inbreuk op de persoonlijke levenssfeer van de overige gebruikers zo klein mogelijk te worden gehouden. In de toestemming voor de verwerving kan hier invulling aan worden gegeven door bijvoorbeeld

[53] Het verwerken van gegevens van personen die geen target zijn kan plaatsvinden op grond van artikel 13, eerste lid, sub e van de Wiv 2002, indien dit noodzakelijk is ter ondersteuning van de goede taakuitvoering. In het post-Madrid wetsvoorstel werd voorzien in een nadere regeling voor de verwerking van dergelijke "gegevensbestanden". *Kamerstukken II* 2005/06, 30 553, nr. 3, Memorie van Toelichting, p. 26.

te bepalen dat na verwerving onverwijld de niet-noodzakelijke gegevens worden verwijderd.

In vier gevallen is de Commissie van oordeel dat de verwerving van bepaalde webfora de proportionaliteitstoets niet kan doorstaan en dat de verwerving daarvan onrechtmatig is. Het betreft hier grotere webfora waarbij het aanwezige aantal targets en de te verwachten opbrengst in geen verhouding staat tot de inbreuk op de persoonlijke levenssfeer van de overige gebruikers. De Commissie acht het verder een tekortkoming dat de verwerving van deze webfora meerdere jaren is voortgezet zonder dat aanwijsbaar op enig moment de noodzaak en proportionaliteit hiervan ter discussie is komen te staan. In de geheime bijlage bij dit rapport specificeert de Commissie deze conclusie.

d) Toestemmingsniveau
In het overgrote gedeelte van de bestudeerde operaties is de toestemming voor de operatie of voor de verlenging van de operatie op het juiste niveau verkregen. Op dit algemene beeld bestaan enkele uitzonderingen.

De Grondwet biedt een bijzondere bescherming aan 'stromende' (*real time*) communicatie. In overeenstemming hiermee dient de minister toestemming te geven voor, bijvoorbeeld, een hack indien daarmee 'stromende' communicatie wordt verworven. Het overgrote deel van de verworven gegevensverzamelingen betreft echter 'opgeslagen' communicatie waarvoor geen bijzonder toestemmingsregime geldt.[54] In één geval heeft de AIVD echter 'live' toegang verkregen tot een gegevensverzameling en heeft op deze wijze 'stromende' communicatie ontvangen. De Commissie acht het evident dat deze activiteit als tap had moeten worden aangemerkt en dat toestemming van de minister benodigd was. Nu deze toestemming niet was verleend, is de Commissie van oordeel dat deze activiteit onrechtmatig was.

Het Mandaatbesluit beperkt het mandaat wanneer zich bijzondere omstandigheden voordoen of wanneer er overwegingen van principiële aard aan de orde zijn. De Commissie is van oordeel dat bij enkele operaties overwegingen van principiële aard aan de orde zijn (geweest). De principiële afwegingen vloeien hier voort uit de aard en omvang van de verworven gegevensverzamelingen en de inbreuk die daarbij wordt gemaakt op de persoonlijke levenssfeer van een groot aantal overige gebruikers. Dit brengt met zich mee dat de uitzonderingsregel van het Mandaatbesluit van toepassing is. Er mag op dit punt alertheid worden verwacht van de AIVD. Gelet op het inbreukmakend karakter had het bij deze specifieke gegevensverzamelingen in de rede gelegen om op een hoger niveau toestemming te verzoeken. Dit is ten onrechte nagelaten en daarmee is onzorgvuldig gehandeld. Het betreft hier overigens operaties die ook elders in dit rapport worden besproken.

e) Zorgvuldigheid
Een nadere invulling van de in acht te nemen zorgvuldigheid is het uitgangspunt dat de AIVD slechts gegevensverzamelingen zal verwerven indien de dienst in staat is deze effectief te bewerken. In de bovengenoemde beleidsnotitie van de AIVD uit 2011 is dit uitgedrukt als het uitgangspunt van *select before you collect.* In één specifiek geval vraagt de Commissie zich af of de AIVD voldoende in staat is, zelfstandig of in samenwerking met buitenlandse diensten, de verworven gegevens voldoende effectief te bewerken. In de geheime bijlage bij dit rapport licht de Commissie dit geval nader toe. De Commissie ziet vooralsnog geen

[54] De aanhangige wijziging van de Grondwet op dit punt zal, indien aangenomen, dit onderscheid tussen 'opgeslagen' en 'stromende' communicatie overigens wegnemen.

aanleiding de verwerving van deze gegevens als onrechtmatig aan te merken, doch beklemtoont de noodzaak tot zorgvuldige afwegingen op dit punt. In het kader van de zorgvuldige taakuitvoering dient de AIVD zich ervan te overtuigen dat alle mogelijke dreigingen tijdig worden onderkend en opgevolgd. Ook het doelmatigheidsoordeel speelt hierbij een rol. Indien vooraf of tijdens een operatie blijkt dat de AIVD zelfstandig of in samenwerking met buitenlandse diensten gegevens onvoldoende kan bewerken, bijvoorbeeld vanwege een gebrek aan vertaalcapaciteit, dan zullen nadrukkelijk andere opties zoals het uitbrengen van een ambtsbericht moeten worden overwogen. Op die wijze worden andere onderdelen van de overheid in staat gesteld om maatregelen te treffen.

f) Gebruik van de gegevens
De Commissie is van oordeel dat de interne werkwijze waarbij ongeëvalueerde gegevens van webfora ter beschikking kunnen worden gesteld voor de uitvoering van andere taken dan de a- of d-taak (veiligheids- of inlichtingentaak) van de AIVD niet rechtmatig is. Het gaat hier om de situatie (zoals omschreven in paragraaf 5.4.1) waarin een operationeel team op verzoek ongeëvalueerde gegevens, waaronder de inhoud van communicatie, verstrekt ten behoeve van een lopend veiligheidsonderzoek op grond van de b-taak (veiligheidsonderzoeken) van de AIVD. In deze gevallen wordt een inbreuk gemaakt op de persoonlijke levenssfeer van de bij het veiligheidsonderzoek betrokken personen waarvoor de wet geen toereikende grondslag biedt.

In algemene zin staat niets in de weg aan de interne verstrekking van gegevens uit operationele onderzoeken ten behoeve van veiligheidsonderzoeken. Artikel 18 van de Wiv 2002 biedt echter geen grondslag voor de inzet van bijzondere bevoegdheden voor de uitvoering van andere taken dan a- of d-taak door de AIVD. De Commissie is van oordeel dat een betrokkene in een veiligheidsonderzoek die in het geheel nog niet in beeld is geweest in enig operationeel onderzoek niet mag worden nageslagen in een systeem waarin ongeëvalueerde gegevens zijn opgeslagen.[55] Een andere situatie doet zich voor indien de AIVD reeds wel onderzoek heeft gedaan naar betrokkene vanuit de a- of d-taak; in dat geval staat niets eraan in de weg om bij een veiligheidsonderzoek acht te slaan op verdere gegevens.

Voor een goed begrip van deze materie merkt de Commissie nog het volgende op. De AIVD verzamelt gegevens voor lopende onderzoeken. De verzamelde gegevens worden na verwerving beoordeeld op relevantie ('bewerken'). Bij gegevensverzamelingen kan hierbij een vorm van metadata-analyse of bestandsvergelijking worden toegepast. De resultaten uit een dergelijke analyse zullen in de regel relevant zijn voor een operationeel onderzoek en verder worden verwerkt. Dit betreft dan ook *geëvalueerde* gegevens. Ten aanzien van de overige gegevens is in dit stadium (nog) niet vastgesteld in hoeverre zij relevant zijn. Daarom dienen deze gegevens naar het oordeel van de Commissie te worden aangemerkt als *ongeëvalueerde* gegevens. Deze mogen niet ter beschikking worden gesteld voor andere dan de a- of d-taak van de dienst.

De Commissie beveelt aan de werkwijze op dit punt te herzien en de mogelijkheid tot het verstrekken van gegevens te beperken tot geëvalueerde gegevens. Zij beveelt aan de mogelijkheid tot naslag door veiligheidsonderzoekers op dit punt ongedaan te maken. De

[55] Dit is in lijn met het oordeel van de Commissie over het gebruik van samengevoegde metagegevens voor andere taken dan de veiligheids- of inlichtingentaak, mede gelet op artikel 35. Toezichtsrapport nr. 38 van de CTIVD, paragrafen 4.3 en 6 (onder 4.2).

Commissie merkt overigens op dat zij vooralsnog de indruk heeft dat van bovenstaande werkwijze slechts zeer beperkt gebruik is gemaakt.

g) Bewaartermijnen
Bij de inzet van andere bijzondere bevoegdheden, zoals een tap, wordt na een bepaalde periode de niet-relevante opbrengst verwijderd en vernietigd. De Commissie heeft in het toezichtsrapport inzake gegevensverwerking van telecommunicatie reeds opgemerkt dat de wet geen bewaartermijnen voorschrijft voor de ongeëvalueerde (ruwe) gegevens, anders dan de regeling voor sigint.[56] Zij heeft in dat rapport de aanbeveling gedaan om dit onderwerp te betrekken bij de eerstvolgende wijziging van de Wiv 2002.

In aanvulling op die aanbeveling merkt de Commissie het volgende op. Ook zonder een nadere wettelijke regeling op dit punt is de AIVD gehouden gegevens te verwijderen die hun betekenis hebben verloren (artikel 43). Bij de initiële verwerving van gegevens kan hiermee rekening worden gehouden, door vooraf te bepalen hoe lang de te verwerven gegevens zullen worden bewaard. Dit gebeurt nu reeds bij de inzet van de tapbevoegdheid, ter invulling van het vereiste van subsidiariteit. Juist ook bij de verwerving van gegevensverzamelingen, zoals webfora, waarbij in sommige gevallen ook gegevens van personen worden verzameld die niet relevant zijn voor enig operationeel onderzoek, is het van belang dat een bewaartermijn wordt vastgelegd.

De Commissie beveelt aan, vooruitlopend op een mogelijke wetswijziging, bewaartermijnen in te voeren voor de ongeëvalueerde gegevens van webfora. Nu dit niet reeds bij de verwerving is bepaald, dient dit alsnog te worden vastgesteld. Indien de ongeëvalueerde gegevens geen betekenis voor lopende onderzoeken meer hebben, dienen deze zoveel als (technisch) mogelijk is te worden verwijderd. Overigens is de Commissie van oordeel dat de AIVD de bestudeerde webfora, uitgezonderd die webfora waarvan in dit toezichtsrapport wordt geoordeeld dat de verwerving onrechtmatig was, heeft mogen bewaren.

h) Bevragingen via menselijke bronnen
Bij bevragingen aan menselijke bronnen in het kader van het verwerven van gegevens van sociale media is naar het oordeel van de Commissie sprake van instructies, zoals deze term in de wet wordt gebruikt. Dat betekent dat deze instructies dienen te worden vastgelegd (artikel 21, zesde lid). Door vast te leggen wat aan een menselijke bron wordt gevraagd en wat vervolgens de opbrengst is, wordt invulling gegeven aan het vereiste van bronvermelding. Ook wordt hierdoor de interne verantwoording van en het extern toezicht op de inzet van de agent gediend. In enkele operaties zijn de bevragingen aan de agent en de opbrengst lange tijd niet structureel vastgelegd. Hierdoor is het niet in alle bestudeerde dossiers mogelijk na te gaan welke gegevens voor welk doel zijn verworven. In 2013 heeft het ondersteunende team dit proces verbeterd en inmiddels wordt van de bevragingen wel aantekening bijgehouden.

De Commissie beveelt aan in het geval gegevensverzamelingen van sociale media via menselijke bronnen worden bevraagd, van elk van deze afzonderlijke bevragingen aantekening bij te houden. De Commissie beveelt voorts aan dat indien een menselijke bron gegevens verzamelt die zijn te vergelijken met verkeers- en gebruikersgegevens, de interne procedure als bij artikel 28 Wiv 2002 wordt gevolgd. Dit betekent dat een gemotiveerd

[56] Alleen voor ruwe gegevens uit de ongerichte interceptie van niet-kabelgebonden communicatie kent de wet een bewaartermijn van een jaar (artikel 27, negende lid). Toezichtsrapport nr. 38 van de CTIVD, paragraaf 6 (onder 4.1).

verzoek om toestemming aan het hoofd van de dienst dient te worden gericht. In deze gevallen behoeven deze bevragingen dan niet ook nog afzonderlijk als instructie te worden vastgelegd en daarvan verslag te worden opgemaakt.

i) Beperkingen uit andere wetgeving
In enkele bestudeerde operaties hebben menselijke bronnen aan de AIVD aangegeven dat zij behoefte aan duidelijkheid hadden over de rechtmatigheid van hun medewerking aan de AIVD. De Wet bescherming persoonsgegevens verbiedt het hen in het algemeen om persoonsgegevens aan derden te verstrekken. In de Wiv 2002 is in verband daarmee een ontheffing gecreëerd voor informanten, die hen bevrijdt van andere wettelijke verplichtingen wanneer zij gegevens verstrekken aan de AIVD (artikel 17, derde lid). In tegenstelling tot de regeling voor informanten, voorziet de wet niet uitdrukkelijk in een dergelijke regeling voor agenten die gegevens verstrekken. De overwegingen van de wetgever die aan de ontheffing voor informanten ten grondslag liggen, doen echter evident ook opgeld voor de situatie waarin agenten zich bevinden.[57] De Commissie is dan ook van oordeel dat deze ontheffing ook geldt voor menselijke bronnen die de dienst aanmerkt als agenten. Agenten mogen dus onder dezelfde voorwaarden als informanten gegevens verstrekken aan de AIVD, ook als hen dat normaal gesproken op grond van privacywetgeving niet zou zijn toegestaan.

5.5 Samenwerking met buitenlandse diensten

5.5.1 Praktijk

Kenmerkend voor sociale media is dat de communicatie niet gebonden is aan landsgrenzen en dat de communicatie dan ook vaak tussen personen in meerdere landen tegelijk plaatsvindt. Voor het onderzoek door de AIVD op sociale media heeft dit verschillende consequenties.

Enerzijds zijn de personen naar wie de dienst onderzoek verricht veelal over grenzen heen verspreid en in meerdere landen actief. Zoals reeds blijkt uit de jaarverslagen van de AIVD zijn veel van de dreigingen die de dienst onderzoekt verbonden met internationaal opererende netwerken en organisaties. In de bestudeerde operaties in dit onderzoek was dit ook het geval. Tevens is het niet altijd kenbaar waar ter wereld een bepaalde persoon op het internet zich bevindt en in hoeverre het relevant is voor de taakstelling van de dienst onderzoek te doen naar die persoon.

Anderzijds raken deze onderzoeken van de AIVD vaak aan de belangen en de rechtsorde van andere landen. De dienst verzamelt ook gegevens die van minder belang zijn voor Nederland, maar soms van groot belang zijn voor een ander land. De omgekeerde situatie komt ook voor. Daar komt bij dat wanneer de dienst op sociale media opereert via agenten, het handelen van deze agenten mogelijk ook een betekenis of gevolg heeft in andere landen. Hier moet ook worden gedacht aan het uitvoeren van een hack op afstand, waarbij de hack in potentie is gericht op een computer in een ander land.[58] Tot slot worden veel vormen van

[57] *Kamerstukken II* 1997/98, 25 877, nr. 3, Memorie van Toelichting, p. 23-24. Zie ook: *Kamerstukken I* 2007/08, 30 553, nr. C, p. 4.
[58] Vergelijk het vraagstuk in verband met het Cybercrime verdrag in verband met het doorzoeken van een computer op afstand. Hierbij is niet altijd bekend of deze zich op Nederlands grondgebied bevindt. *Kamerstukken II* 2004-05, 30 036, nr. 2, p. 9 en *Kamerstukken II* 2012/13, 28 684, nr. 363.

sociale media door buitenlandse bedrijven ontwikkeld, waardoor de AIVD afhankelijk is van de medewerking van buitenlandse diensten voor het verkrijgen van gegevens.

De hiervoor beschreven situatie geldt niet alleen voor de AIVD, maar voor vele buitenlandse diensten. In de bestudeerde onderzoeken is dan ook telkens een sterk wederzijds belang te zien bij de samenwerking met buitenlandse diensten in verband met sociale media. Ook is in deze onderzoeken een intensivering van die internationale samenwerking te zien. De samenwerking krijgt op verschillende wijzen gestalte, onder meer via de uitwisseling van persoonsgegevens, waaronder gegevensverzamelingen zoals webfora, en de afstemming van operationele onderzoeken.

Zoals is aangestipt zijn aanbieders van sociale media geregeld buiten Nederland gevestigd. Dit betekent dat ook de gegevensverzamelingen vaak buiten Nederland zijn gelegen. Dit beperkt uiteraard de mogelijkheden voor de AIVD om zelfstandig bevragingen bij deze aanbieders te kunnen uitvoeren. Net als iedere gebruiker van sociale media, is het de AIVD bekend in welk land een bepaalde aanbieder van sociale media is gevestigd. Om met succes gegevens te kunnen verzamelen kan de AIVD verzoeken doen aan de collegadienst in dat land. Zoals in paragraaf 5.4 reeds voor de Nederlandse situatie is beschreven, staan ook aan een buitenlandse dienst meerdere wegen ter beschikking om opgeslagen gegevens te verzamelen. Bovendien kan de buitenlandse dienst andere bevoegdheden hebben.[59] De AIVD heeft in de regel geen zicht op de wijze waarop de buitenlandse dienst de verzochte gegevens heeft verzameld.

In het kader van agentenoperaties op sociale media vindt met regelmaat samenwerking plaats met buitenlandse diensten. Door samenwerking kan bij de operaties rekening worden gehouden met de belangen van die landen en kan tijdig duidelijk worden gemaakt welke dienst welke personen in onderzoek heeft. Bovendien kan op deze manier worden voorkomen dat een buitenlandse dienst nodeloos aandacht besteed bij zijn onderzoeken aan een persoon, die uiteindelijk een agent van de AIVD blijkt te zijn. In enkele gevallen noopt het internationale karakter van sociale media tot verdergaande afstemming met buitenlandse diensten over de inzet en aandachtsgebieden van agenten.

Naast (target)gerichte verzoeken wisselt de AIVD op beperkte schaal ook gegevensverzamelingen van sociale media uit. Hierbij moet in de eerste plaats gedacht worden aan de samenwerking met betrekking tot webfora. Deze praktijk is reeds in algemene zin aan de orde geweest in het toezichtsrapport inzake gegevensverwerking van telecommunicatie.[60] In het kader van dit onderzoek heeft de Commissie nader bezien of de uitwisseling van de webfora in de onderzoeksperiode rechtmatig is geschied.

5.5.2 Bevindingen

De Commissie voert reeds een ander diepteonderzoek uit naar samenwerking van de AIVD met buitenlandse diensten in de volle breedte.[61] Dit onderzoek is daarom in de eerste plaats gericht op het uitwisselen van gegevensverzamelingen *van* sociale media en de afstemming van operationele onderzoeken *op* sociale media. Voorts is aandacht besteed aan de vraag of

[59] De Commissie heeft in het toezichtsrapport over gegevensverwerking van telecommunicatie uiteengezet hoe de AIVD (en MIVD) met de verschillen in bevoegdheden wordt omgesprongen. Toezichtsrapport nr. 38 van de CTIVD, paragraaf 5.1.
[60] Idem, paragraaf 5.6.
[61] Aangekondigd op 27 maart 2013.

er sprake is van omzeiling van de beperkingen in de eigen bevoegdheden bij de samenwerking met buitenlandse diensten.

De Commissie heeft geen aanwijzingen dat de AIVD bij de bevragingen de buitenlandse dienst verzoekt om middelen in te zetten waar de AIVD niet over beschikt. De bevragingen die in de bestudeerde onderzoeken zijn aangetroffen verhouden zich naar hun aard en omvang telkens goed tot de eigen bevoegdheden van de AIVD.

Betreffende operaties die de AIVD samen met buitenlandse diensten heeft uitgevoerd, heeft de Commissie geen onrechtmatigheden geconstateerd. Hier wordt over het algemeen zorgvuldig en bedachtzaam te werk gegaan, en hiervan wordt in voldoende mate verslag bijgehouden. In één geval heeft de AIVD de *nicknames* van agenten medegedeeld aan de buitenlandse dienst. De Commissie heeft er in algemene zin begrip voor dat het nodig kan zijn om aan een buitenlandse dienst een zekere mate van openheid te geven over de inzet van agenten, zeker waar dit de inzet op sociale media betreft. In dit bijzondere geval is zij niettemin van oordeel dat hiertoe geen noodzaak bestond. De Commissie beveelt aan, mede gelet op artikel 15, strikt de hand te houden aan de bronbescherming.

De Commissie is van oordeel dat het delen van webfora met buitenlandse diensten in vrijwel alle onderzochte gevallen rechtmatig is geschied. De enige uitzondering wordt hierna toegelicht. De Commissie herhaalt de aanbeveling uit haar toezichtsrapport over gegevensverwerking van telecommunicatie om bij de verwerving van een webforum via een buitenlandse dienst vast te leggen waarom het gerechtvaardigd is kennis te nemen van de inhoud van het webforum.[62]

De onderzoeken van de AIVD in het kader van zijn veiligheidstaak (a-taak) zijn juist waar het sociale media betreft zeer sterk verweven met de binnenlandse veiligheid van andere landen. Wanneer de AIVD de beschikking heeft over een grote hoeveelheid gegevens die in potentie raakt aan de veiligheid van andere landen, dan getuigt het van zorgvuldigheid dat samenwerking wordt gezocht. Hier is ook sprake van een inspanningsverplichting om tot een zorgvuldige en tijdige duiding van de beschikbare gegevens te komen. Deze inspanningsverplichting vindt niet alleen een grondslag in de eigen taakstelling van de AIVD maar ook in het internationaal en Europees recht. Nederland heeft vele verdragen geratificeerd en politieke verklaringen ondertekend waarmee het zich heeft verplicht tot samenwerking bij het voorkomen van terrorisme.[63]

De Commissie tekent hierbij het volgende aan. De samenwerking met buitenlandse diensten geschiedt op basis van gelijkwaardigheid en iedere dienst heeft daarbij eigen prioriteiten. Dit brengt met zich mee dat het delen van de webfora met enkele buitenlandse diensten nog niet automatisch betekent dat er dan van uit mag worden gegaan dat de verworven gegevens daarmee voldoende worden geanalyseerd. Iedere dienst kijkt immers slechts naar de voor hem relevante targets. Indien goede afspraken ontbreken, wordt het risico onvoldoende uitgesloten dat relevante informatie niet wordt opgemerkt en in het uiterste geval een aanslagplan onopgemerkt blijft. De Commissie beveelt aan om bij de samenwerking met buitenlandse diensten zoveel mogelijk te komen tot een werkverdeling.

---

[62] Toezichtsrapport nr. 38 van de CTIVD, paragraaf 6 (onder 3.5).

[63] Bijvoorbeeld: Verdrag van de Raad van Europa ter voorkoming van terrorisme, *Trb.* 2006, 34. Raad van Ministers van de OVSE, *Decision 7/06 Countering the use of the internet for terrorist purposes*, 5 december 2006. Raad van de Europese Unie, *The EU Counter-terrorism strategy*, 30 november 2005 (14469/4/05, aangenomen op 15/16 december 2005) en opvolgende conclusies van de Raad.

Er is een lange periode onvoldoende bijgehouden met welke diensten welke webfora werden gedeeld. Het is een wettelijk vereiste dat van de verstrekking van persoonsgegevens aantekening wordt bijgehouden (artikel 42). Bovendien heeft de beperkte verslaglegging erin geresulteerd dat de voor het onderzoek inzake gegevensverwerking van telecommunicatie[64] aan de Commissie verstrekte informatie op dit punt onvolledig was. In het toen door de AIVD verstrekte overzicht ontbraken vijf gevallen waarin webfora zijn verstrekt. De Commissie is overigens van oordeel dat de AIVD deze vijf extremistische webfora rechtmatig verstrekte aan de betreffende buitenlandse diensten. Voor de inhoud of conclusies van het onderzoek naar gegevensverwerking van telecommunicatie heeft het ontbreken van deze informatie dan ook geen gevolgen gehad.

Voor de beantwoording van de vraag of een bijzondere bevoegdheid ten behoeve van de eigen taken wordt ingezet of ten behoeve van een buitenlandse dienst, is doorslaggevend of er hierdoor een directe bijdrage wordt geleverd aan een lopend onderzoek.[65] In een aantal gevallen heeft het verwerven van bepaalde webfora niet direct bijgedragen aan enig lopend onderzoek van de AIVD en lag de nadruk op het belang van de buitenlandse dienst. In deze gevallen verzamelde de AIVD gegevens over buitenlandse extremistische of terroristische organisaties waarnaar de dienst zelf geen lopende onderzoeken had. Nu de webfora niet zijn verworven voor eigen lopende onderzoeken, moet de verwerving van deze webfora worden aangemerkt als het verlenen van ondersteuning aan de betreffende buitenlandse diensten. De Commissie is van oordeel dat vanwege het ontbreken van de toestemming van de minister op grond van artikel 59, vijfde lid, in elk geval in vier gevallen onrechtmatig is gehandeld. De Commissie merkt ten overvloede op dat zij niet de indruk heeft dat in deze gevallen werd beoogd het wettelijk toestemmingsregime te omzeilen. De onrechtmatigheid berust op een, naar het oordeel van de Commissie, verkeerde interpretatie van het onderscheid tussen verwerving ten behoeve van *eigen* lopende onderzoeken en verwerving ter *ondersteuning* van een buitenlandse dienst. De Commissie hecht eraan, in lijn met haar eerdere toezichtsrapporten, dit onderscheid strikt te hanteren.

Tot slot heeft de AIVD een webforum voor een buitenlandse dienst verzameld, waarbij de Commissie niet overtuigd is dat de verwerving van dit forum proportioneel was. Er bestonden in dit geval bij de buitenlandse dienst wel aanwijzingen tegen een van de beheerders van het forum, doch de Commissie acht dit onvoldoende om de inbreuk op de persoonlijke levenssfeer van de gebruikers van dat forum te rechtvaardigen. Hierbij weegt de Commissie in overwegende mate mee dat het forum op zichzelf geen radicaal signatuur had. In de toestemming op grond waarvan het forum is verworven, is in het geheel geen aandacht besteed aan deze aspecten. De Commissie acht daarom de verwerving en de daaropvolgende verstrekking van dit forum aan de buitenlandse dienst onrechtmatig. In de geheime bijlage gaat de Commissie nader in op dit geval.

[64] Toezichtsrapport nr. 38 van de CTIVD.
[65] 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. 50 (bijlage), paragraaf 8.2.

6. Conclusies en aanbevelingen

De AIVD heeft de afgelopen jaren veel geïnvesteerd in het onderzoek op sociale media. Het is de Commissie uit het dossieronderzoek gebleken dat de door de AIVD gepleegde investeringen om adequaat gebruik te maken van het internet ten aanzien van de taakuitvoering vruchten afwerpen en het onderzoek op sociale media onderdeel wordt van het vaste instrumentarium van de dienst. Doordat de ontwikkelingen op het vlak van sociale media zeer snel gaan, vraagt het een voortdurende grote inspanning van de dienst om hiermee in de pas te blijven lopen.

De Wet op de inlichtingen- en veiligheidsdiensten 2002 is geschreven in een tijd dat sociale media nog niet die maatschappelijke rol hadden die zij inmiddels vervullen. In algemene zin constateert de Commissie dat het onderzoek op sociale media zich goed verhoudt tot de kaders die de huidige wet stelt. De wet biedt ook naar Europese maatstaven voldoende waarborgen. Op enkele specifieke punten zoals de bewaartermijnen van ruwe gegevens en metadata-analyse behoeft het wettelijk kader echter aanvulling, zoals de Commissie reeds in het toezichtsrapport over gegevensverwerking van telecommunicatie heeft aanbevolen.[66]

De digitale context waarbinnen de onderzoeken van de AIVD plaatsvinden zorgt er wel voor dat het interne beleid op verschillende terreinen geregeld aanpassing behoeft opdat de waarborgen voor de bescherming van de persoonlijke levenssfeer betekenisvol worden ingevuld. De Commissie constateert dat met regelmaat zich (technische) mogelijkheden voordoen waarvoor nog geen beleid is ontwikkeld en die zich niet altijd laten vergelijken met andere werkwijzen. Bij dit pionieren op het vlak van nieuwe mogelijkheden mag van de direct betrokken medewerkers een voortdurende alerte houding worden verwacht. Principiële vragen dienen tijdig te worden onderkend en op het juiste niveau te worden besproken.

Organisatorische inbedding (paragaaf 5.1)

6.1 De AIVD volgt de ontwikkelingen op het vlak van sociale media op de voet en speelt daar actief op in. (paragraaf 5.1)

Passief onderzoek op sociale media (paragraaf 5.2)

6.2 Veel gegevens op sociale media zijn voor een ieder vrij raadpleegbaar, en kunnen worden getypeerd als open bronnen. (paragraaf 5.2.1)

6.3 De Commissie constateert dat de AIVD slechts beperkt via directe toegang tot internet gegevens op sociale media verzamelt. Over het algemeen verzamelen de operationele teams via andere wegen gegevens van sociale media, dan daar zelf op internet naar te zoeken. De weinige aangetroffen resultaten blijven ruimschoots binnen de grenzen van de algemene bevoegdheid tot het verzamelen van gegevens en zijn zorgvuldig verwerkt. De resultaten geven geen blijk van dermate intensief of langdurig onderzoek via het internet dat aanvullende lastgeving noodzakelijk is. Ook zijn er geen aanwijzingen dat de gepleegde zoekslagen een meer dan geringe inbreuk op de persoonlijke levenssfeer maken, en daarmee raken aan de bevoegdheid tot observatie. (paragraaf 5.2.2)

[66] Toezichtsrapport nr. 38 van de CTIVD, paragraaf 6 (onder 3.3 en 4.1).

6.4 Onder omstandigheden kan echter ook bij onderzoek in open bronnen een verdergaande inbreuk op de persoonlijke levenssfeer van betrokkenen worden gemaakt. Zo zal in bepaalde gevallen het stelselmatig naslaan van een persoon in open bronnen als observeren moeten worden aangemerkt. De Commissie stelt vast dat er op dit moment geen richtlijnen bestaan binnen de dienst aan de hand waarvan kan worden vastgesteld of voor een verdergaand of langdurig internetonderzoek een toestemming tot observatie moet worden aangevraagd. (paragraaf 5.2.2)

6.5 **De Commissie beveelt aan een heldere maatstaf vast te leggen wanneer voor een verdergaand of langdurig internetonderzoek een toestemming tot observatie moet worden aangevraagd.** (paragraaf 5.2.2)

6.6 De Commissie acht het van belang dat de grens tussen de algemene bevoegdheid tot gegevensverwerving en de inzet van een agent op grond van artikel 21 Wiv 2002 wordt bewaakt. Die grens wordt overschreden indien een medewerker van de dienst zich actief opstelt en interactie aangaat met anderen, ook als dit slechts gebeurt om niet op te vallen. In dat geval is er sprake van opereren onder dekmantel volgens artikel 21. De Commissie constateert dat het onderscheid tussen de algemene bevoegdheid tot gegevensverwerving en de inzet van agenten in het huidige beleid voldoende gewaarborgd is. (paragraaf 5.2.2)

6.7 De Commissie acht het onwenselijk en onwerkbaar voor de AIVD om alle waarnemingen op het internet vast te leggen, maar meent wel dat relevante resultaten dienen te worden gedocumenteerd. Wanneer resultaten onvoldoende worden gedocumenteerd zijn deze niet raadpleegbaar voor andere dienstmedewerkers en neemt de controleerbaarheid van de producten van de AIVD af. (paragraaf 5.2.2)

6.8 **De Commissie beveelt aan dat de dienst het bestaande beleid voor het operationeel gebruik van internet en het vastleggen van resultaten nader formuleert. Het onderzoek op internet op basis van de algemene bevoegdheid tot het verzamelen van gegevens dient helder te worden afgebakend ten opzichte van de meer inbreukmakende bijzondere bevoegdheden en dient te worden voorzien van eenduidige regels voor de registratie van onderzoeksresultaten.** (paragraaf 5.2.2)

6.9 De Commissie merkt op dat andere sectoren van de maatschappij laten zien dat de mogelijkheden op het gebied van geautomatiseerde systemen voor het verzamelen van gegevens van het internet snel toenemen. Er bestaan inmiddels verschillende instrumenten voor sociale netwerkanalyse en het monitoren van evenementen. (paragraaf 5.2.2)

6.10 **De Commissie beveelt aan dat de dienst bij het ontwikkelen van nieuwe onderzoeksmethoden op het vlak van sociale media, in een vroeg stadium de kennis uit andere sectoren van de maatschappij en uit de wetenschap op het vlak van (privacy-) waarborgen benut. Op deze wijze wordt bevorderd dat nieuwe systemen vanaf ingebruikname aan alle wettelijke vereisten voldoen.** (paragraaf 5.2.2)

Actief onderzoek op sociale media (paragraaf 5.3)

6.11 De AIVD zet agenten in om op sociale media gegevens te verzamelen. Dit betreffen zowel eigen medewerkers als niet-medewerkers (externe agenten). (paragraaf 5.3.1)

6.12 De inzet van *externe* agenten op sociale media gebeurt zorgvuldig en doordacht. De verslaglegging van sturing en de verzamelde gegevens is afdoende. (paragraaf 5.3.2)

6.13 **Wel beveelt de Commissie aan om de online identiteiten van de agenten steeds zorgvuldig vast te leggen. Dit is van belang voor de veiligheid van de agent en controleerbaarheid van de operatie.** (paragraaf 5.3.2)

6.14 De Commissie is kritisch ten aanzien van de inzet van *eigen* medewerkers van de AIVD als agent op het internet. Er ligt een richtinggevend intern beleidskader voor deze operaties. In de praktijk wordt hier echter onvoldoende de hand aan gehouden. Alle bestudeerde operaties schieten met name tekort op het punt van effectieve verslaglegging. In vijf gevallen is dit tekortschieten van dien aard dat de Commissie dit als onrechtmatig beoordeelt. In deze operaties zijn weinig tot geen operatierapporten opgesteld, waarmee de transparantie en controleerbaarheid van deze operaties in het gedrang is gekomen. Door het ontbreken van effectieve verslaglegging is het onderzoek van de Commissie bemoeilijkt. (paragraaf 5.3.2)

6.15 **De Commissie beveelt aan de verslaglegging van de lopende operaties onverwijld in lijn te brengen met de binnen de dienst gebruikelijke standaarden.** (paragraaf 5.3.2)

6.16 In één operatie is de toestemming voor de inzet van een eigen medewerker als agent ongedateerd. De Commissie beoordeelt dit als een onzorgvuldigheid die ertoe leidt dat niet kan worden vastgesteld of toestemming bij aanvang van de operatie aanwezig was. (paragraaf 5.3.2)

6.17 De Commissie stelt vast dat het ontbreken van de betrokkenheid van een acquisiteur of een andere vorm van begeleiding heeft bijgedragen aan de door de Commissie geconstateerde tekortkomingen op het gebied van verslaglegging. Dit probleem is reeds bij een interne evaluatie door de AIVD opgemerkt. (paragraaf 5.3.2)

6.18 **De Commissie beveelt aan de begeleiding van de medewerkers-agenten op het internet aanzienlijk te verbeteren en bij dit traject de vraag te betrekken hoe de sturing en interne verantwoording van deze operaties kan worden verbeterd.** (paragraaf 5.3.2)

6.19 Onder strikte voorwaarden kunnen agenten toestemming krijgen strafbare feiten te plegen. Dit kan ook noodzakelijk zijn bij operaties op het internet, opdat een agent niet uit de toon valt. In enkele operaties is aan de agent daarom toestemming gegeven strafbare feiten te plegen. In twee gevallen is de toestemming (veel) te laat voorgelegd aan het diensthoofd ter goedkeuring. De Commissie is van oordeel dat dit formele tekortkomingen betreffen. De later afgegeven toestemmingen herstellen naar het oordeel van de Commissie niet dat hier onzorgvuldig is gehandeld. (paragraaf 5.3.3)

6.20 **In een andere operatie beveelt de Commissie aan alsnog te bezien of een toestemming voor het plegen van strafbare feiten dient te worden aangevraagd. De agent begeeft zich met zijn uitlatingen op het internet mogelijk over de grens van wat toelaatbaar is ingevolge de strafwet.** (paragraaf 5.3.3)

6.21 De Commissie constateert dat in de door haar bestudeerde operaties, op één uitzondering na, er telkens van is afgezien om de Landelijk Officier van Justitie (LOvJ) in kennis te stellen van de toestemming strafbare feiten te plegen. De Commissie wijst erop dat volgens het interne beleid de LOvJ in beginsel in kennis dient te worden gesteld van een toestemming tot het plegen van strafbare feiten. In het in juni 2014 verschenen toezichtsrapport inzake enkele langlopende agentenoperaties heeft de Commissie aanbevolen de LOvJ te informeren over *alle* toestemmingen voor het plegen van misdrijven. (paragraaf 5.3.3)

6.22 In de operaties waarin géén toestemming voor het plegen van strafbare feiten is gegeven, dienen de agenten binnen de grenzen van de strafwet te blijven. Bij *externe* agenten ziet de acquisiteur daar op toe. De Commissie is van oordeel dat de acquisiteurs in de bestudeerde operaties hier voldoende invulling aan geven. (paragraaf 5.3.3)

6.23 In vier van de vijf onder 6.16 genoemde operaties is een toestemming strafbare feiten gegeven. Het tekortschieten in de verslaglegging bij deze operaties betekent ook dat ten aanzien van het plegen van strafbare feiten niets is vastgelegd. Deze tekortkoming is van dien omvang dat hier sprake is van een onrechtmatigheid bij de uitvoering van de toestemming tot het plegen van strafbare feiten. Door een gebrek aan verslaglegging valt voor de Commissie niet te beoordelen of aan deze agenten voldoende sturing is gegeven dan wel voldoende is toegezien op het naleven van het verbod op uitlokking. (paragraaf 5.3.3)

Onderzoek door het verwerven van gegevensverzamelingen van sociale media (paragraaf 5.4)

6.24 Aanbieders van sociale media houden vaak gegevensverzamelingen aan met daarin gebruikersgegevens en inhoud van communicatie. De AIVD kan via hacks, agenten of buitenlandse diensten geheel of gedeeltelijk toegang proberen te verkrijgen tot deze gegevensverzamelingen. Daarbij kunnen (target)gerichte bevragingen worden uitgevoerd. In sommige gevallen is het toegestaan om een gehele gegevensverzameling te verwerven (bijvoorbeeld een jihadistisch webforum).

6.25 De door de Commissie bestudeerde hacks die door de AIVD zijn uitgevoerd om webfora te verwerven zijn in alle gevallen goed gemotiveerd. De gehackte webfora waren telkens als geheel relevant voor de taakuitvoering van de AIVD, en de toestemming voor de hack is in het algemeen gegeven op het daartoe bevoegde beslisniveau. In enkele gevallen is door een unithoofd toestemming gegeven voor een hack op afstand, terwijl dit op het niveau van de directeur had moeten gebeuren. De Commissie acht dit onzorgvuldig. (paragraaf 5.4.2, onder a)

6.26 De menselijke bronnen (informanten en/of agenten) die gegevensverzamelingen verwerven of die (target)gerichte bevragingen uitvoeren, worden voornamelijk door het ondersteunende team ingezet. Sinds begin 2013 is in het geheel geen afweging meer gemaakt van de proportionaliteit van de inzet van deze bronnen. (paragraaf 5.4.2, onder b)

6.27 De Commissie is ten aanzien van vijf agentenoperaties van oordeel dat de motivering van de inzet van de desbetreffende agenten dermate tekortschiet dat de toestemmingen hiervoor onrechtmatig zijn gegeven. Dit heeft tot gevolg gehad dat er meerdere webfora zijn verworven terwijl bij aanvang geen zorgvuldige afweging van

noodzakelijkheid, proportionaliteit en subsidiariteit was vastgelegd. (paragraaf 5.4.2, onder b)

6.28 In maart 2013 is door de dienst een intern voorstel opgesteld om de motivering van de lasten te verbeteren, maar de uitvoering van dit voorstel is in de onderzoeksperiode niet ter hand genomen, zodat het geconstateerde gebrek in de motiveringen bleef voortbestaan. De AIVD heeft aangegeven dat de werkwijzen kort geleden zijn aangepast, hetgeen nog wel moet worden vertaald in de interne beleidsregels. De Commissie is van mening dat van de dienst een alertere houding op dit punt had mogen worden verwacht. (paragraaf 5.4.2, onder b)

6.29 **De Commissie beveelt aan dat de AIVD op korte termijn de aangepaste werkwijzen in het beleid vastlegt.** (paragraaf 5.4.2, onder b)

6.30 De Commissie constateert dat de afdeling juridische zaken van de AIVD in 2011 een gedegen beleidsnotitie over het verwerven van gegevensverzamelingen in het algemeen heeft opgesteld, waarin de relevante waarborgen een plaats hebben. De implementatie hiervan is echter niet ter hand genomen. (paragraaf 5.4.2, onder c)

6.31 **De Commissie beveelt aan dat de AIVD op korte termijn bindend beleid vaststelt op het punt van de verwerving van gegevensverzamelingen (waaronder webfora).** (paragraaf 5.4.2, onder c)

6.32 De Commissie heeft de verwerving van de webfora in de onderzoeksperiode bestudeerd. De Commissie stelt vast dat in vrijwel alle gevallen webfora betreft waarvan de verwerving noodzakelijk was voor de taakuitvoering van de dienst. (paragraaf 5.4.2, onder c)

6.33 In vier gevallen is de Commissie echter van oordeel dat deze verwerving van webfora niet voldoet aan het beginsel van proportionaliteit en dat deze verwerving onrechtmatig was. Het betreft hier grotere webfora waarbij het aanwezige aantal targets en de te verwachten opbrengst van relevante gegevens in geen verhouding staat tot de inbreuk op de persoonlijke levenssfeer van de overige gebruikers. De Commissie acht het verder een tekortkoming dat de verwerving van deze webfora meerdere jaren is voortgezet zonder dat aanwijsbaar op enig moment de noodzaak en proportionaliteit hiervan ter discussie is komen te staan. (paragraaf 5.4.2, onder c)

6.34 In het overgrote deel van de bestudeerde operaties is de toestemming op het juiste niveau verkregen. Op dat algemene beeld bestaan enkele uitzonderingen. In één geval kreeg de AIVD *real time* gegevens binnen, net als bij een tap. Omdat toestemming van de minister ontbrak, is de Commissie van oordeel dat deze activiteit onrechtmatig was. (paragraaf 5.4.2, onder d)

6.35 De Commissie wijst er verder op dat het Mandaatbesluit voorschrijft toestemming op een hoger niveau te vragen voor de inzet van bijzondere bevoegdheden indien er overwegingen van principiële aard aan de orde zijn. De Commissie is van oordeel dat dit ten onrechte is nagelaten bij de verwerving van enkele gegevensverzamelingen, aangezien een principiële afweging had moeten worden gemaakt nu hierbij ook inbreuk werd gemaakt op de persoonlijke levenssfeer van een groot aantal overige gebruikers. Door na te laten op een hoger niveau toestemming te vragen, heeft de dienst onzorgvuldig gehandeld. (paragraaf 5.4.2, onder d)

6.36 De gegevens(verzamelingen) van sociale media die de AIVD verwerft moeten zorgvuldig worden verwerkt. Dit houdt mede in dat de AIVD zich er van te voren rekenschap van moet geven of de dienst in staat is, alleen of in samenwerking met andere diensten, de gegevens effectief te bewerken. (paragraaf 5.4.2, onder e)

6.37 In één specifiek geval vraagt de Commissie zich af of de AIVD voldoende in staat is, zelfstandig of in samenwerking met buitenlandse diensten, de verworven gegevens voldoende effectief te bewerken. De Commissie ziet vooralsnog geen aanleiding de verwerving van deze gegevens als onrechtmatig aan te merken, doch beklemtoont de noodzaak tot zorgvuldige afwegingen op dit punt. (paragraaf 5.4.2, onder e)

6.38 De AIVD mag gegevens die door middel van de inzet van bijzondere bevoegdheden voor de veiligheids- of inlichtingentaak zijn verzameld ook gebruiken voor andere taken, zoals de uitvoering van veiligheidsonderzoeken. De Commissie is van oordeel dat dit alleen geldt voor *geëvalueerde gegevens.* De interne werkwijze waarbij medewerkers in het kader van de b-taak (veiligheidsonderzoeken) van de AIVD kennis kunnen nemen van deze gegevens acht de Commissie in strijd met artikel 18 Wiv 2002 en derhalve onrechtmatig. De Commissie merkt overigens op dat zij vooralsnog de indruk heeft dat van bovenstaande werkwijze slechts zeer beperkt gebruik is gemaakt. (paragraaf 5.4.2, onder f)

6.39 **De Commissie beveelt aan de werkwijze op dit punt te herzien en de mogelijkheid tot het verstrekken van gegevens te beperken tot geëvalueerde gegevens. Zij beveelt aan om de mogelijkheid tot naslag door veiligheidsonderzoekers op dit punt ongedaan te maken.** (paragraaf 5.4.2, onder f)

6.40 Zoals de Commissie reeds in het toezichtsrapport inzake gegevensverwerking van telecommunicatie heeft opgemerkt, schrijft de wet geen bewaartermijnen voor ten aanzien van ongeëvalueerde (ruwe) gegevens, anders dan de regeling voor sigint. De Commissie wijst erop dat ook zonder een nadere wettelijke regeling op dit punt, de AIVD gehouden is gegevens te verwijderen en te vernietigen indien deze hun betekenis hebben verloren. (paragraaf 5.4.2, onder g)

6.41 **De Commissie beveelt aan, vooruitlopend op een mogelijke wetswijziging, bewaartermijnen in te voeren voor de ongeëvalueerde gegevens van webfora. Indien de ongeëvalueerde gegevens geen betekenis voor lopende onderzoeken meer hebben, dienen deze zoveel als (technisch) mogelijk is te worden verwijderd.** (paragraaf 5.4.2, onder g)

6.42 De Commissie is overigens van oordeel dat de AIVD de bestudeerde webfora, voor zover de verwerving daarvan door de Commissie niet onrechtmatig is geoordeeld, tot op heden heeft mogen bewaren. (paragraaf 5.4.2, onder g)

6.43 De (target)gerichte bevragingen voor gegevens van sociale media aan menselijke bronnen zijn in enkele operaties lange tijd niet structureel vastgelegd. Hierdoor is het niet in alle bestudeerde dossiers mogelijk na te gaan welke gegevens voor welk doel zijn verworven. (paragraaf 5.4.2, onder h)

6.44 **De Commissie beveelt aan in het geval gegevensverzamelingen via menselijke bronnen worden bevraagd, van elk van deze afzonderlijke bevragingen aantekening bij te houden.** (paragraaf 5.4.2, onder h)

6.45 **De Commissie beveelt aan dat indien een menselijke bron gegevens verzamelt die zijn te vergelijken met verkeers- of gebruikersgegevens, de interne procedure als bij artikel 28 Wiv 2002 wordt gevolgd. Dit betekent dat een gemotiveerd verzoek om toestemming aan het hoofd van de dienst dient te worden gevraagd.** (paragraaf 5.4.2, onder h)

6.46 In de Wiv 2002 is een ontheffing gecreëerd voor informanten, die hen bevrijdt van andere wettelijke verplichtingen wanneer zij gegevens verstrekken aan de AIVD. In tegenstelling tot de regeling voor informanten voorziet de wet niet nadrukkelijk in een regeling voor agenten die gegevens verstrekken. Omdat de overwegingen van de wetgever die aan de ontheffing voor informanten ten grondslag liggen ook evident opgeld doen voor de situatie waarin agenten zich bevinden, is de Commissie van oordeel dat deze ontheffing ook geldt voor agenten. Agenten mogen dus onder dezelfde voorwaarden als informanten gegevens verstrekken aan de AIVD. (paragraaf 5.4.2, onder i)

Samenwerking met buitenlandse diensten (paragraaf 5.5)

6.47 De internationale context van sociale media dwingt de AIVD tot samenwerking met buitenlandse diensten. De Commissie constateert dat hierbij grote wederzijdse belangen aanwezig zijn. (paragraaf 5.5.1)

6.48 De Commissie heeft bij dit diepteonderzoek geen aanwijzingen dat door de AIVD eigen bevoegdheden worden omzeild bij de bevragingen van sociale media via buitenlandse diensten. Ook gaat de dienst zorgvuldig en bedachtzaam te werk waar eigen onderzoeken ten aanzien van sociale media worden afgestemd met buitenlandse diensten. (paragraaf 5.5.2)

6.49 **De Commissie beveelt wel aan om strikt de hand te houden aan de bronbescherming waar het gaat om het delen van *nicknames* van eigen agenten met buitenlandse diensten.** (paragraaf 5.5.2)

6.50 **De Commissie beveelt aan, zoals zij reeds in haar toezichtsrapport over gegevensverwering van telecommunicatie deed, om bij de verwerving van een webforum via een buitenlandse dienst vast te leggen waarom het gerechtvaardigd is kennis te nemen van de inhoud van het webforum.** (paragraaf 5.5.2)

6.51 Wanneer de AIVD de beschikking heeft over een grote hoeveelheid gegevens die in potentie raakt aan de veiligheid van andere landen, dan getuigt het van zorgvuldigheid dat samenwerking wordt gezocht. Hier is ook sprake van een inspanningsverplichting om tot een zorgvuldige en tijdige duiding van de beschikbare gegevens et komen. Het delen van de webfora met enkele buitenlandse diensten betekent niet automatisch dat er van uit mag worden gegaan dat de verworven gegevens daarmee voldoende worden geanalyseerd. Indien goede afspraken ontbreken, wordt het risico onvoldoende uitgesloten dat relevante informatie niet wordt opgemerkt en in het uiterste geval een aanslagplan onopgemerkt blijft. (paragraaf 5.5.2)

6.52 **De Commissie beveelt aan bij de samenwerking met buitenlandse diensten zoveel mogelijk te komen tot een werkverdeling bij het bewerken van de webfora.** (paragraaf 5.5.2)

6.53 De AIVD wisselt enkele webfora uit met buitenlandse diensten. Als een dergelijk webforum niet direct bijdraagt aan enig lopend onderzoek van de AIVD dan moet de verwerving als ondersteuning aan een buitenlandse dienst worden aangemerkt. Dit betekent dat de minister toestemming dient te geven voor de verwerving van een dergelijk forum ten behoeve van de buitenlandse dienst. De Commissie is van oordeel dat in vier gevallen onrechtmatig is gehandeld omdat de toestemming van de minister ontbrak. (paragraaf 5.5.2)

6.54 In één ander dan de hiervoor gemelde gevallen is de Commissie van oordeel dat de verwerving in het geheel niet had mogen plaatsvinden omdat de verwerving niet voldeed aan het proportionaliteitsvereiste. De Commissie is van oordeel dat dit forum onrechtmatig is verworven. (paragraaf 5.5.2)

Aldus vastgesteld in de vergadering van de Commissie d.d. 16 juli 2014.

CTIVD nr. 39

BIJLAGE

Overzicht van het toetsingskader bij het toezichtsrapport inzake onderzoek door de AIVD op sociale media

Om op een toegankelijke wijze een overzicht te geven van het toetsingskader worden hierna de verschillende methodes om onderzoek te doen op sociale media geduid met de bijbehorende vereisten uit de Wiv 2002. De genoemde methodes worden in paragraaf 5 nader uitgewerkt. Hier zij benadrukt dat dit overzicht niet uitputtend is, maar dat hiermee bedoeld is het toetsingskader op een beknopte wijze weer te geven.

Passief onderzoek op sociale media

Vereiste	*Uitwerking*
Grondslag	Artikelen 6 en 12 Wiv 2002
Definitie	Onderzoek op open bronnen
Toestemming	Geen
(Vorm)vereisten	- uitoefening voor een bepaald doel, slechts voor zover noodzakelijk (12) - behoorlijkheid, zorgvuldigheid, bron- of betrouwbaarheidsvermelding (12)
Begrenzing	- gegevens van derden slechts betrekken indien noodzakelijk (13) - meer dan geringe inbreuk op grondrechten, zoals de persoonlijke levenssfeer, onder meer te toetsen aan de intentie, de aard van de methoden en de opslag van gegevens - stelselmatig (target-)gericht onderzoek (20) - opereren onder dekmantel (21)

Observatie van personen op sociale media

Vereiste	*Uitwerking*
Grondslag	Artikel 20 Wiv 2002
Definitie	Persoonsgericht onderzoek dat naar duur, plaats, intensiteit, frequentie of hulpmiddelen als stelselmatig moet worden aangemerkt
Toestemming	Door teamhoofd
(Vorm)vereisten	- uitoefening voor een bepaald doel, slechts voor zover noodzakelijk (12) - behoorlijkheid, zorgvuldigheid, bron- of betrouwbaarheidsvermelding (12) - motivering (20) - verslaglegging (33)
Begrenzing	- gegevens van derden slechts betrekken indien noodzakelijk (13) - noodzakelijkheid, proportionaliteit en subsidiariteit (18, 31, 32)

Actief onderzoek door agenten op sociale media

Vereiste	*Uitwerking*
Grondslag	Artikel 21 Wiv 2002
Definitie	Opereren met agenten op sociale media, eventueel met gebruik van dekmantel
Toestemming	Door directeur of unithoofd, verlenging door teamhoofd
(Vorm)vereisten	- uitoefening voor een bepaald doel, slechts voor zover noodzakelijk (12) - behoorlijkheid, zorgvuldigheid, bron- of betrouwbaarheidsvermelding (12)

	- motivering - verslaglegging (21, zesde lid, 33)
Begrenzing	- noodzakelijkheid, proportionaliteit en subsidiariteit (18, 31, 32) - verbod op instigatie: 'Tallon-criterium' (21, lid 4) - veiligheid van de agent (15) - strafbare feiten alleen met toestemming en instructie aanwezig is (21, lid 3)

Verwerving van gegevensverzamelingen van sociale media

Vereiste	***Uitwerking***
Grondslag	Artikelen 17, 21, 24, 59 Wiv 2002
Definitie	De verzameling van (gedeelten van) gegevensverzamelingen van sociale media
Toestemming	Afhankelijk van de bevoegdheid
(Vorm)vereisten	- uitoefening voor een bepaald doel, slechts voor zover noodzakelijk (12) - behoorlijkheid, zorgvuldigheid, bron- of betrouwbaarheidsvermelding (12) - motivering (21, 24) - verslaglegging (33)
Begrenzing	- gegevens van derden slechts betrekken indien noodzakelijk (13) - proportionaliteit en subsidiariteit (31, 32) - noodzakelijk voor de a- of d-taak, tenzij artikel 17 de grondslag vormt (18)

Ontsluiten en bewaren van gegevensverzamelingen van sociale media

Vereiste	***Uitwerking***
Grondslag	Artikelen 6 en 12 Wiv 2002
Definitie	Analyseren, ontsluiten, bewaren van de gegevens
(Vorm)vereisten	- uitoefening voor een bepaald doel, slechts voor zover noodzakelijk (12) - behoorlijkheid, zorgvuldigheid, bron- of betrouwbaarheidsvermelding (12) - beveiliging van gegevens, o.m. tegen onbevoegde verwerking (16) - autorisatiebeleid (16, 35) - verwijderen en vernietigen wanneer gegevens betekenis verliezen (43) - *de Commissie heeft eerder aanbevolen om bij wet in bewaartermijnen te voorzien voor ruwe gegevens alsmede in een regeling voor de verwerking van metagegevens*
Begrenzing	- gegevens van derden slechts betrekken indien noodzakelijk (13) - noodzakelijk voor de a- of d-taak, tenzij de gegevens op grond van artikel 17 zijn verworven (18)

Uitwisselen van gegevensverzamelingen van sociale media

Vereiste	***Uitwerking***
Grondslag	Artikelen 36 *of* 59 Wiv 2002
Definitie	Verstrekken van gegevensverzameling aan een buitenlandse dienst en/of ontvangen van gegevensverzameling van een buitenlandse dienst
Toestemming	Door teamhoofd of unithoofd (36) *of* minister (59)
(Vorm)vereisten	- uitoefening voor een bepaald doel, slechts voor zover noodzakelijk (12) - behoorlijkheid, zorgvuldigheid, bron- of betrouwbaarheidsvermelding (12) - aantekening bijhouden (42) - derdepartijregel (37)
Begrenzing	- noodzakelijk voor de eigen taak (36) *of* - in het belang dat de buitenlandse dienst behartigt (59)

(Persoons)gericht bevragen van gegevensverzamelingen van sociale media

Vereiste	*Uitwerking*
Grondslag	Artikelen 17, 21 en 59 Wiv 2002
Definitie	(Target)gericht zoeken in gegevensverzameling via menselijke bronnen of buitenlandse diensten
(Vorm)vereisten	- uitoefening voor een bepaald doel, slechts voor zover noodzakelijk (12) - behoorlijkheid, zorgvuldigheid, bron- of betrouwbaarheidsvermelding (12) - vastleggen instructie aan agent (21, zesde lid) - motiveren indien gelijk te stellen met artikel 28
Begrenzing	- proportionaliteit en subsidiariteit (31, 32) - noodzakelijk voor de a- of d-taak, tenzij artikel 17 de grondslag vormt (18)