Bijlage I
Toetsingskader

Bij het toezichtsrapport Automated OSINT: tools en bronnen voor openbronnenonderzoek

CTIVD nr. 74

Vastgesteld op 22 december 2021

CTIVD
Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten

Commissie van Toezicht
op de Inlichtingen- en
Veiligheidsdiensten

CTIVD nr. 74

TOETSINGSKADER

Automated OSINT: tools en bronnen voor openbronnenonderzoek

Inhoudsopgave

CTIVD nr. 74

TOETSINGSKADER

Automated OSINT: tools en bronnen voor openbronnenonderzoek

1. Inleiding

Het onderliggende toetsingskader heeft betrekking op 'automated Open Source Intelligence' (hierna: automated OSINT). Voor OSINT wordt ook wel de Nederlandse term 'openbronnenonderzoek' gebruikt of, in juridische terminologie, 'het verzamelen van gegevens uit voor een ieder toegankelijke informatiebronnen' (met behulp van een technisch hulpmiddel). Wanneer openbronnenonderzoek geautomatiseerd plaatsvindt met behulp van specialistische software of webapplicaties, is er sprake van automated OSINT.

Onder de Wiv 2017 is OSINT een algemene bevoegdheid van de diensten, waarbij er een onderscheid is tussen niet-stelselmatige en stelselmatige inzet (artikel 25 en 38 Wiv 2017 respectievelijk). Bij het stelselmatig verzamelen van gegevens omtrent een persoon uit voor een ieder toegankelijke informatiebron is toestemming vereist. Openbronnenonderzoek en de bevoegdheid tot het stelselmatig verzamelen van gegevens omtrent een persoon uit voor een ieder toegankelijke informatiebronnen onderscheidt zich van de bijzondere bevoegdheden, waarvoor de minister van Binnenlandse Zaken en Koninkrijksrelaties (BZK) of van Defensie of namens deze het hoofd van de dienst toestemming moet verlenen en de algemene vereisten voor de inzet van bijzondere bevoegdheden uit artikel 29 Wiv 2017 gelden. De diensten moeten bij de verwerking van gegevens te allen tijde de algemene bepalingen omtrent gegevensverwerking in acht nemen.

Dit toetsingskader schetst de eisen waaraan die praktijk dient te voldoen op basis van de Wiv 2017, de wetsgeschiedenis en overige bronnen. Deze bijlage is als volgt opgebouwd. Hoofdstuk 2 bespreekt de wettelijke grondslag voor de verwerking van gegevens bij automated OSINT. Hoofdstuk 3 gaat over de aangelegen bevoegdheden van observatie en de inzet van agenten. Hoofdstuk 4 behandelt de algemene bepalingen omtrent gegevensverwerking bij de inzet van tools voor automated OSINT. Hoofdstuk 5 biedt een overzicht van de wettelijke vereisten waaraan de CTIVD in dit rapport de praktijk toetst.

2. Grondslag voor het verzamelen van gegevens

De grondslag voor het verzamelen van gegevens door middel van automated OSINT is te vinden in de algemene bevoegdheid van de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) en de Militaire Inlichtingen- en Veiligheidsdienst (MIVD) om gegevens te verzamelen uit een voor een ieder toegankelijke informatiebron (artikel 25 lid 1 sub a Wiv 2017) of de bevoegdheid voor het stelselmatig verzamelen van gegevens omtrent een persoon uit een voor een ieder toegankelijke informatiebron (artikel 38 Wiv 2017).

Het verzamelen van gegevens uit voor een ieder toegankelijke bronnen betreft in beide gevallen een 'algemene bevoegdheid'. Dit betekent dat gegevens uit een voor ieder toegankelijke informatiebron kunnen worden verwerkt voor elke taak van de AIVD en de MIVD. Deze taken staan omschreven in artikel 8 Wiv 2017 voor de AIVD en artikel 10 Wiv 2017 voor de MIVD. Zij kunnen dus ook een rol spelen bij veiligheidsonderzoeken ter uitvoering van de Wet veiligheidsonderzoeken (Wvo), het opstellen van dreigings- en risicoanalyses en het bewaken en beveiligen van gegevens door de AIVD en de MIVD.[1]

Het hoofdstuk is als volgt opgebouwd. Paragraaf 1 gaat over de reikwijdte van het begrip 'voor een ieder toegankelijke informatiebron'. Paragraaf 2 gaat over het verzamelen van 'commercieel beschikbaar gestelde gegevens' en paragraaf 3 gaat over de bevoegdheid van het stelselmatig verzamelen van persoonsgegevens uit voor een ieder toegankelijke informatiebronnen.

2.1 Reikwijdte definitie 'voor een ieder toegankelijke informatiebron'

De term 'open bron' wordt in de memorie van toelichting van de WIv 2017 (en in dit rapport) gebruikt als synoniem voor 'voor een ieder toegankelijke informatiebron'.[2] Het verzamelen van gegevens uit voor een ieder toegankelijke informatiebronnen valt onder de algemene bevoegdheid in artikel 25 lid 1 sub a Wiv 2017. In de memorie van toelichting wordt 'een voor ieder toegankelijk informatiebron' als volgt omschreven:

"Het gaat hier om alle bronnen (traditionele media, internet e.d.) die zonder meer kunnen worden geraadpleegd en waarvoor geen drempels bestaan".[3]

De wetgever legt in de wetsgeschiedenis echter niet uit wat als een 'drempel' moet worden gezien. Wel wordt duidelijk gemaakt dat de diensten (uiteraard) kennis mogen nemen van gegevens uit kranten en tijdschriften, klaarblijkelijk ook als daarvoor registratie en betaling is vereist.[4] Ook staat in de memorie van toelichting dat medewerkers van de diensten gegevens kunnen verzamelen van 'openbaar toegankelijke delen van Facebook, Twitter en Linkedin', op grond van artikel 25 lid 1 sub a Wiv 2017, voor zover dat niet stelselmatig is.[5] Als gegevens worden verzameld van '*gesloten* delen van sociale media', moet de agentbevoegdheid worden toegepast.[6] Dat wil in deze context zeggen dat een persoon of medewerker van de dienst wordt aangestuurd om via een sociale mediadienst gegevens te verzamelen voor de taakuitvoering van de AIVD of de MIVD. Met de agentbevoegdheid is het ook mogelijk 'vrienden te worden' met een target op een sociale mediadienst en gegevens op gesloten delen van een profiel te verzamelen (zie verder paragraaf 3.2).

1 *Kamerstukken II* 2016/17, 34588, nr. 3, p. 42.
2 Zie, o.a., *Kamerstukken II* 2016/17, 34588, nr. 3, p. 55.
3 *Kamerstukken II* 2016/17, 34588, nr. 3, p. 38.
4 Zie, o.a., *Kamerstukken II* 2016/17, 34588, nr. 3, p. 63.
5 *Kamerstukken II* 2016/17, 34588, nr. 3, p. 39 en 55-56.
6 Idem, p. 63.

Op basis van de wetsgeschiedenis van de Wiv 2017 zijn de diensten bevoegd een (nep)profiel op een sociale mediadienst aan te maken, waarmee medewerkers vervolgens publiek toegankelijke gegevens mogen verzamelen. In eerdere toezichtsrapporten heeft de CTIVD hetzelfde geconcludeerd.[7] Ook voor opsporingsdiensten, waarbij openbronnenonderzoek door het Wetboek van Strafvordering wordt gereguleerd, is het toegestaan een (nep)profiel aan te maken, waarna medewerkers, net als alle andere gebruikers, een website kunnen betreden en kennis mogen nemen van de inhoud daarvan.[8] Afhankelijk van de werkwijze bij het verzamelen van gegevens na het aanmaken van een account of profiel, moet ook aan de inzet van bijzondere bevoegdheden door de AIVD en de MIVD worden gedacht, zoals observatie (paragraaf 3.1) en de agentbevoegdheid (paragraaf 3.2).

Voor de nadere inkadering van het begrip 'voor een ieder toegankelijke informatiebron' zoekt de CTIVD aansluiting bij het Wetboek van Strafvordering, waarin openbronnenonderzoek door de politie wordt gereguleerd. De laatst beschikbare memorie van toelichting uit het Wetboek van Strafvordering hiervoor dateert alweer uit 1997.[9] De Commissie 'Strafvordering in het digitale tijdperk', onder voorzitterschap van prof. Koops (hierna: Commissie-Koops), heeft in 2018 in opdracht van de regering onderzoek gedaan naar (onder andere) openbronnenonderzoek op internet. Naar aanleiding van het rapport van de Commissie-Koops wordt in het Wetboek van Strafvordering een nieuwe bijzondere opsporingsbevoegdheid voorgesteld voor het stelselmatig overnemen van persoonsgegevens uit publiek toegankelijke bronnen (net zoals de algemene bevoegdheid van de AIVD en de MIVD in artikel 38 Wiv 2017). Er is nog geen wetsvoorstel waarin dit geregeld wordt. Wel bestaat er een zogenoemde 'ambtelijke versie' (hierna 'voorontwerp'). Dit voorontwerp geeft breed gedeelde inzichten weer over openbronnenonderzoek.

In de memorie van toelichting bij het voorontwerp voor een nieuw Wetboek van Strafvordering wordt gespecifieerd dat ook 'bronnen die publiekelijk toegankelijk zijn, waarbij wel sprake is van enige beperking wat betreft het geven van toegang, maar geen effectieve controle plaatsvindt bij het verstrekking van toegang', als een 'voor een ieder toegankelijke informatiebron' worden aangemerkt.[10] Een beperking kan bestaan uit de verplichting tot registratie van een account, alvorens van gegevens kennis kan worden genomen. Voor de reikwijdte van het begrip open bron wordt daarmee aangehaakt bij de strafbaarstelling van computervredebreuk in artikel 138ab van het Wetboek van Strafrecht.[11] Bij een niet-toegankelijke bron moet er een minimale vorm van toegangscontrole zijn, die meer is dan een "pro-forma"-beveiliging die bestaat uit een (virtueel) bordje "verboden toegang".[12]

Bij het raadplegen van een voor een ieder toegankelijke informatiebron kan geen sprake zijn van het doorbreken of ontwijken van beveiliging, het aanwenden van een technische ingreep, valse signalen of valse sleutel om toegang te krijgen tot de bron. Het feit dat bepaalde inhoud zich niet laat indexeren door een zoekmachine uit praktische of commerciële overwegingen, of dat in de algemene voorwaarden staat dat de inhoud bestemd is voor een bepaalde kring van personen, maar waarbij de beperking niet door een feitelijke toegangscontrole wordt bewerkstelligd, wordt niet gezien als een 'drempel'. Er is daarbij nog steeds sprake van een 'open bron'. Het 'deep web' – het gedeelte van het internet dat niet geïndexeerd is door de voor het reguliere internet gebruikelijke zoekmachines, maar dat wel feitelijk toegankelijk is als men de website bezoekt – is dus ook een open bron, omdat het geen minimaal niveau van beveiliging kent. Ook het 'dark web', het gedeelte van het internet waar de IP-adressen van genetwerkte computers verborgen zijn door middel van speciale software zoals

7 Zie toezichtsrapport nr. 39 (2014) over de rechtmatigheid van het onderzoek op sociale media door de AIVD en toezichtsrapport nr. 55 (2018) over door derden op internet aangeboden bulkdatasets.
8 Zie memorie van toelichting bij het wetsvoorstel tot vaststelling van het nieuwe Wetboek van Strafvordering (juli 2020, ambtelijke versie), p. 499.
9 *Kamerstukken II* 1996/97, nr. 3, p. 26-27.
10 Zie memorie van toelichting bij het wetsvoorstel tot vaststelling van het nieuwe Wetboek van Strafvordering (juli 2020, ambtelijke versie), p. 498 en p. 499.
11 Idem, p. 498.
12 Idem.

The Onion Router (Tor), wordt als een 'voor een ieder toegankelijke informatiebron' gezien, omdat er geen toegangscontrole plaatsvindt en iedereen de benodigde software kan downloaden en gebruiken.[13]

2.2 Verzamelen van commercieel beschikbaar gestelde gegevens

De AIVD en de MIVD zijn bevoegd tot het verzamelen van 'commercieel beschikbaar gestelde gegevens' op grond van artikel 25 lid 1 sub b Wiv 2017. Dit zijn gegevens waartoe men slechts na betaling toegang krijgt. De memorie van toelichting bij de Wiv 2017 geeft als voorbeeld 'de gegevens van de Kamer van Koophandel'.[14]

In het Wetboek van Strafvordering wordt het verzamelen van commercieel beschikbaar gestelde gegevens als een 'publiek toegankelijke bron' gezien.[15] De financiële drempel die bestaat voor toegang tot gegevens van bijvoorbeeld LexisNexis, de Kamer van Koophandel, en 'integrale bestanden die op de markt tegen betaling beschikbaar zijn' is daarbij niet relevant. Ook wanneer de financiële drempel zodanig is dat niet iedereen het zich zou kunnen veroorloven.[16]

In de Wiv 2017 vallen commercieel beschikbaar gestelde gegevens, waartoe men slechts tegen betaling toegang krijgt, onder een andere categorie dan gegevens uit een voor een ieder toegankelijke informatiebron; dit in tegenstelling tot de regeling in het voorontwerp van het Wetboek van Strafvordering.

De benaming van de categorie 'informatiebronnen waarvoor aan de dienst een recht op kennisneming is verleend' (artikel 25 lid 1 sub b Wiv 2017), waar dus ook commerciële gegevens onder vallen, doelt op gegevens waarbij aan de diensten een *wettelijk* recht op toegang is verleend, zoals politiegegevens op grond van artikel 17 en 24 van de Wet politiegegevens.[17] In het toezichtsrapport merkt de CTIVD op, dat de wettelijke grondslag voor het verzamelen van commercieel beschikbare gegevens niet voldoende voorzienbaar is voor burgers en de wetgever hier meer duidelijkheid over moet geven met gepaste waarborgen (zie aanbeveling 1 van het toezichtsrapport).

Het verschil in de wettelijke grondslag in de Wiv 2017 brengt echter geen rechtsgevolg met zich mee, omdat artikel 25 lid sub a en sub b Wiv 2017 beiden een algemene bevoegdheid betreffen. Hierbij zijn geen nadere vereisten gesteld voor de inzet van de bevoegdheid, zoals toestemming van het hoofd van de dienst.

De samengestelde datasets met gelekte gegevens die door een commerciële dienstverlener worden aangeboden hebben in de voorkomende gevallen de kenmerken van een bulkdataset, oftewel een set van gegevens waarvan het merendeel van de personen in een dataset niet onder de aandacht van de diensten staat en ook nooit zal staan. In rapport nr. 55 (2018) over door derden aangeboden bulkdatasets op internet rapporteerde de CTIVD over de rechtmatigheid van het verzamelen van deze bulkdatasets op basis van de informantenbevoegdheid (artikel 39 Wiv 2017). De AIVD en de MIVD hebben voor de de verzameling van bulkdatasets een beleid ontwikkeld, waarbij een schriftelijke toets op de beginselen van noodzakelijkheid, proportionaliteit en subsidiariteit wordt uitgevoerd en het hoofd van de dienst of de voor de dienst verantwoordelijke minister om toestemming wordt gevraagd.

13 Idem, p. 499. Zie ook toezichtsrapport nr. 55 (2018).
14 *Kamerstukken II* 2016/17, 34588, nr. 3, p. 38.
15 Memorie van toelichting bij het wetsvoorstel tot vaststelling van het nieuwe Wetboek van Strafvordering (juli 2020, ambtelijke versie), p. 499. In rapport nr. 55 (2018) heeft de CTIVD het kopen van op internet aangeboden bulkdatasets door een persoon eerder gekwalificeerd als de inzet van de informantenbevoegdheid, waarbij op basis van beleid van de diensten extra vereisten golden bij de inzet, zoals toestemming van het hoofd van de dienst of de minister en technische en personele maatregelen werden genomen bij de verdere verwerking van de gegevens.
16 Idem, p. 499.
17 *Kamerstukken II* 2016/17, 34588, nr. 3, p. 38.

Daarnaast is een ministeriële regeling gepubliceerd over de verdere verwerking van gegevens uit bulkdatasets onder de Wiv 2017.[18] Bij automated OSINT verzamelen de diensten zelf geen datasets in hun geheel, om deze daarna te kunnen koppelen aan andere datasets of deze intern te kunnen bevragen. In plaats daarvan worden datasets bij een commerciële dienstverlener (middels een individuele zoekslag) geraadpleegd. Hiermee kan de situatie ontstaan dat verschillende waarborgen van toepassing zijn op wat in beginsel vergelijkbare situaties zijn. Het bovenstaande laat onverlet dat de CTIVD ook toetst aan de algemene vereisten omtrent gegevensverwerking en de eisen van noodzakelijkheid, proportionaliteit, subsidiariteit en gerichtheid.[19]

De *aard* van de gegevens die door de diensten worden verwerkt, kunnen bovendien van invloed zijn op het proportionaliteitsbeginsel in artikel 18 Wiv 2017 (zie paragraaf 4.1). Onder andere uit Europese jurisprudentie over de verwerking van locatiegegevens door inlichtingen- en veiligheidsdiensten is duidelijk dat de verwerking van locatiegegevens een meer ernstige inbreuk op het recht op bescherming van persoonsgegevens en privacy met zich meebrengt.[20] Ook de verwerking van gegevens uit gelekte datasets brengt een grotere inbreuk op fundamentele rechten met zich mee dan bijvoorbeeld de verwerking van gegevens uit voor een ieder toegankelijke nieuwsberichten.[21] De strafbaarstelling in Nederland voor het beschikbaar stellen van niet-openbare gegevens en heling van gegevens per 1 maart 2019, is indicatief voor hoe wordt gekeken naar het overnemen van gegevens uit gelekte datasets.[22] Een en ander heeft invloed op de proportionaliteitstoets bij de verwerking van deze gegevens.

2.3 'Stelselmatig' openbronnenonderzoek

Openbronnenonderzoek wordt door de wetgever niet als een ernstige inbreuk op de fundamentele rechten beschouwd. Het verzamelen van gegevens uit een voor eenieder toegankelijke informatiebron, het verzamelen van commercieel beschikbaar gestelde gegevens, en het stelselmatig verzamelen van persoonsgegevens uit voor ieder toegankelijke informatiebronnen zijn om deze reden in de Wiv 2017 geregeld als algemene bevoegdheden.[23] Aan algemene bevoegdheden zijn minder zware waarborgen gekoppeld dan aan bijzondere bevoegdheden.

Desondanks kan openbronnenonderzoek tot een meer dan geringe inbreuk op de persoonlijke levenssfeer leiden. In de Wiv 2017 is daarom de bevoegdheid van artikel 38 Wiv 2017 ingevoerd, dat de diensten legitimeert tot het *stelselmatig* verzamelen van persoonsgegevens uit een voor eenieder toegankelijke informatiebron.[24] De AIVD en de MIVD kunnen op basis van deze algemene bevoegdheid stelselmatig gegevens omtrent een persoon verzamelen.

---

18 Regeling van de Minister van Binnenlandse Zaken en Koninkrijksrelaties en de Minister van Defensie van 3 november 2020, nr. 2020-0000611095, houdende nadere regels met betrekking tot enkele aspecten van de werkwijze inzake de verdere verwerking van bulkdatasets verworven door de AIVD en MIVD op grond van de Wiv 2017 (Tijdelijke regeling verdere verwerking bulkdatasets Wiv 2017), *Stcrt*. 2020, 56482.

19 Reactie CTIVD op publicatie Tijdelijke regeling verdere verwerking bulkdatasets Wiv 2017 van 5 november 2020.

20 Zie bijvoorbeeld EHRM 8 februari 2018, 31446/12, ECLI:CE:ECHR:2018:0208JUD00314412 *(Ben Faiza/Frankrijk)* en HvJ EU 6 oktober 2020, C-511/18 en C-520/18, ECLI:EU:C:2020:791 (*La Quadrature du Net e.a./Premier ministre e.a.*) en HvJ EU 6 oktober 2020, C-623/17, ECLI:EU:C:2020:790 (*Privacy International/Secretary of State for Foreign and Commonwealth Affairs e.a.*).

21 In het Toetsingskader bij rapport nr. 55 (2018) over door derden op internet aangeboden bulkdatasets wordt ook opgemerkt dat het relevant is voor de ernst van de privacy-inbreuk als een dataset door middel van een strafbaar feit, zoals hacken (computervredebreuk (artikel 138ab Sr)), in de openbaar is gekomen.

22 Per 1 maart 2019 is de Wet computercriminaliteit III in werking getreden (*Stb*. 2019, 67). Artikel 138c stelt het opzettelijk en wederrechtelijk overnemen of doorgeven van gegevens uit een niet-openbare bron strafbaar en artikel 139g Sr stelt heling van gegevens strafbaar.

23 *Kamerstukken II* 2015/17, 34588, nr. 3, p. 55.

24 Deze bepaling is ook ingevoerd ook ter uitvoering van een aanbeveling in de 'Privacy Impact Assessment Wiv 20XX' (Koops e.a., 'Privacy Impact Assessment Wet op de Inlichtingen- en veiligheidsdiensten 20XX', TNO/PILab/Tilburg University 2016.

De aanvraag tot de inzet van de bevoegdheid moet voldoen aan de vereisten van noodzakelijkheid, proportionaliteit, subsidiariteit en gerichtheid (artikel 26 Wiv 2017). Van de inzet van de bevoegdheid moet aantekening worden gehouden (artikel 31 Wiv 2017). Voor de inzet moet toestemming worden verkregen van de minister van BZK of de minister van Defensie, of van het hoofd van de AIVD of de MIVD. Het hoofd van de dienst kan medewerkers aanwijzen die namens hem toestemming mogen verlenen. Met andere woorden: mandatering van het geven van toestemming voor de inzet van de bevoegdheid is mogelijk. De bevoegdheid kan voor een periode van ten hoogste drie maanden worden ingezet. Deze geldingsduur heeft betrekking op de termijn waarbinnen het verzamelen van gegevens uit voor een ieder toegankelijke informatiebronnen kan plaatsvinden. De inzet van de bevoegdheid kan op verzoek worden verlengd.

Wanneer de gegevens op 'stelselmatige wijze' worden verzameld, vindt een meer dan geringe inmenging in de rechten en vrijheden van de betrokkene plaats.[25] In de wetsgeschiedenis van de Wiv 2017 wordt het begrip 'stelselmatigheid' niet gedefinieerd. Voor de invulling van het begrip 'stelselmatigheid' bij het verzamelen van gegevens uit voor een ieder toegankelijke informatiebron sluit de CTIVD aan bij het strafvorderlijk begrip stelselmatigheid, net als zij eerder in onderzoeken naar OSINT heeft gedaan.[26]

In de context van openbronnenonderzoek wordt het begrip nader ingevuld in de memorie van toelichting bij het voorontwerp voor wijziging van boek 2 van het Wetboek van Strafvordering. In deze toelichting wordt verduidelijkt dat de uitoefening van de bevoegdheid stelselmatig is als bij het overnemen van gegevens uit een voor een ieder toegankelijke informatiebron 'op voorhand redelijkerwijs voorzienbaar is dat een min of meer volledig beeld van bepaalde aspecten van het persoonlijk leven van de betrokkene kan worden verkregen'.[27] De vraag of het onderzoek stelselmatig is, moet op voorhand worden beantwoord op basis van de op dat moment beschikbare informatie en de beoogde inzet van het middel, met inachtneming van de ervaringen met resultaten van de inzet van een dergelijk middel in eerdere gevallen.[28]

Het criterium stelselmatigheid bij openbronnenonderzoek krijgt een andere invulling dan stelselmatigheid bij observatie in de fysieke wereld, waarvoor het criterium in het Wetboek van Strafvordering oorspronkelijk is ontwikkeld. In de memorie van toelichting van het voorontwerp worden de volgende factoren geformuleerd om te bepalen of het onderzoek stelselmatig is:

- De omvang en het type van de over te nemen gegevens. Dat wil zeggen de hoeveelheid gegevens, aard van de gegevens en de diversiteit van de gegevens;
- De aard van de bron. Het maakt uit of de gegevens expliciet zijn bedoeld voor een brede verspreiding of niet zijn verspreid met het oog op kennisneming door een brede kring;
- De wijze van zoeken. Het is van belang of de gegevens handmatig worden opgezocht of gebruik wordt gemaakt van een tool voor het geautomatiseerd zoeken en combineren van gegevens. De specificering van de zoekvraag is daarbij ook relevant (wordt bijvoorbeeld een algemene of specifieke vraag gesteld?);
- De opslag en het gebruik van de gegevens en de mogelijke gevolgen voor de persoon. Het maakt uit welke selectiviteit wordt gehanteerd bij het overnemen van de gegevens uit een publiek toegankelijke bron (breed en weinig selectief overnemen van gegevens in interne systemen versus beperkt en gericht overnemen van gegevens).[29]

25 *Kamerstukken II* 2016/17, 34588, nr. 3, p. 63 en *Kamerstukken II* 2016/17, 34588, nr. 18, p. 53. Zie ook, o.a., EHRM 4 mei 2000, nr. 28341/95, ECLI:CE:ECHR:2000:0504JUD002834195, par. 43 (*Rotaru/Roemenië*).
26 Zie ook toezichtsrapport nr. 39 (2014). De voorgestelde bevoegdheid in het Wetboek van Strafvordering is identiek aan de bevoegdheid in de Wiv 2017. Om deze reden wordt aangesloten bij het wetsvoorstel tot vaststelling van het nieuwe Wetboek van Strafvordering.
27 Memorie van toelichting bij het wetsvoorstel tot vaststelling van het nieuwe Wetboek van Strafvordering, juli 2020, p. 499.
28 Idem, p. 500.
29 Idem, p. 501.

In de memorie van toelichting van het voorontwerp wordt terecht opgemerkt dat het gebruik van een tool om op geautomatiseerde wijze gegevens te verzamelen uit voor een ieder toegankelijke informatiebron, de verzameling van gegevens niet per definitie stelselmatig van karakter maakt.[30] Afhankelijk van de omstandigheden van het geval is het verzamelen en overnemen van gegevens met een tool voor automated OSINT stelselmatig. Bovenstaande factoren – die niet als volledig of uitputtend zijn bedoeld - kunnen helpen richting te geven aan de invulling van het criterium stelselmatigheid in het kader van de Wiv 2017.

30 Idem, p. 502.

3. Aangelegen bevoegdheden bij openbronnen-onderzoek

Bij openbronnenonderzoek gaat het in beginsel om het verzamelen van *historische gegevens*, zoals de berichten die door een target van de AIVD of de MIVD op een voor eenieder toegankelijke plek in het verleden op internet zijn geplaatst.[31] Openbronnenonderzoek waarbij het doel is gegevens in (near) real time in de toekomst te verzamelen of waarbij met andere inlichtingenmiddelen gegevens worden verzameld over een target van internet, kunnen er toe leiden dat bijzondere bevoegdheden moeten worden ingezet. De twee bijzondere bevoegdheden die daarvoor in het bijzonder kunnen worden ingezet betreffen observatie (artikel 40 Wiv 2017, paragraaf 3.1) en de inzet van agenten (artikel 41 Wiv 2017, paragraaf 3.2).

3.1 Observatie

Observatie betreft het observeren en volgen van natuurlijke personen of zaken (artikel 40 Wiv 2017).[32] Bij onderzoek naar targets via internet kan er bijvoorbeeld sprake zijn van observatie als regelmatig (dus met tussenpozen) of continu (zonder tussenpozen) de gedragingen van een target op sociale mediadiensten (zoals Twitter en Facebook) worden geraadpleegd.[33]

Bij de inzet van observatie als bijzondere bevoegdheid gaat het om *toekomstgericht* onderzoek.[34] De minister van BZK of Defensie kan toestemming geven voor de inzet van de bijzondere bevoegdheid, waarbij "doormandatering" mogelijk is.[35] Als toestemming wordt verleend, is vanaf dat moment observatie mogelijk tot een periode van maximaal drie maanden. Verlenging van deze periode is mogelijk.[36]

Het observeren of volgen van personen is een bijzondere bevoegdheid. Als gevolg daarvan moet de inzet voldoen aan de algemene vereisten bij de inzet van bevoegdheden (artikel 26 en artikel 29 Wiv 2017) en moet in de aanvraag worden gemotiveerd waarom de inzet noodzakelijk, proportioneel, subsidiair, en zo gericht mogelijk wordt geacht.[37]

De gegevens die worden verzameld door middel van observatie dienen zo spoedig mogelijk en maximaal binnen één jaar op relevantie worden beoordeeld (waarbij deze toets na toestemming van het hoofd van de dienst voor zes maanden kan worden uitgesteld). Gegevens die niet relevant zijn voor het onderzoek, of enig ander lopend onderzoek, moeten terstond worden vernietigd (artikel 27 Wiv 2017). Voor gegevens die door middel van een algemene bevoegdheid worden verzameld, dus ook voor OSINT, geldt geen voorgeschreven termijn voor het op relevantie beoordelen van de gegevens. Deze moeten worden verwijderd als ze niet meer van betekenis zijn (zie paragraaf 4.3).

31 *Kamerstukken II* 2016/17, 34588, nr. 3, p. 63-64.
32 *Kamerstukken II* 2016/17, 34588, nr. 3, p. 62.
33 *Kamerstukken II* 2016/17, 34588, nr. 3, p. 62. Zie ook toezichtsrapport nr. 39 (2014).
34 *Kamerstukken II* 2016/17, 34588, nr. 18, p. 53.
35 Artikel 40 lid 2 Wiv 2017.
36 Artikel 29 lid 1 Wiv 2017.
37 Zie ook artikel 29 lid 2 Wiv 2017 voor overige vereisten.

3.2 De agentbevoegdheid

De agent is een natuurlijk persoon die doelbewust door de dienst wordt ingezet om gericht gegevens te verzamelen die voor de taakuitvoering van de AIVD of de MIVD van belang zijn.[38] Een agent kan een medewerker van de dienst zijn, maar ook een derde.

Bij openbronnenonderzoek is de inzet van de agentbevoegdheid (artikel 41 Wiv 2017) bijvoorbeeld op zijn plaats als een medewerker van de AIVD of de MIVD, of een derde, door middel van een (nep)profiel gegevens verzamelt op gesloten delen van sociale media.[39] Daarmee kan bijvoorbeeld door middel van een 'nepaccount' gepoogd worden vrienden te worden met een target om daarmee toegang te krijgen tot gegevens in een profiel op een sociale mediadienst die niet voor iedereen toegankelijk is, maar alleen voor vrienden.[40] Ook de interactie met een persoon onder een dekmantel (zoals een nepprofiel) op online fora of een online chatdienst kan worden gebaseerd op de agentbevoegdheid of de informantenbevoegdheid (artikel 39 Wiv 2017).[41]

De minister van BZK of van Defensie, of het hoofd van de AIVD of van de MIVD, moet toestemming geven voor de inzet van de bijzondere bevoegdheid.[42] In de aanvraag moet worden gemotiveerd waarom de inzet voldoet aan de beginselen van noodzakelijkheid, gerichtheid, proportionaliteit en subsidiariteit.[43] Het is mogelijk dat de persoon op basis van een schriftelijke instructie handelingen verricht die tot gevolg hebben dat een strafbaar feit wordt gepleegd.[44] De natuurlijke persoon mag bij de uitvoering van de instructie een persoon niet brengen tot het beramen of plegen van een ander strafbaar feit, dan waarop diens optreden van tevoren was verricht (het uitlokkingsverbod).[45] De inzet van de agentbevoegdheid mag voor maximaal een jaar worden aangevraagd, waarbij telkens een verlenging van een jaar mogelijk is. Deze periode is langer dan de gebruikelijke periode van drie maanden, omdat agentoperaties doorgaans een langere duur kennen.[46]

38 Zie artikel 41 Wiv 2017 en *Kamerstukken II* 2016/17, 34588, nr. 3, p. 64.
39 *Kamerstukken II* 2016/17, 34588, nr. 3, p. 63. Zie ook toezichtsrapport nr. 39 (2014), p. 10 en p. 35.
40 Zie de Memorie van toelichting bij het wetsvoorstel tot vaststelling van het nieuwe Wetboek van Strafvordering (juli 2020, ambtelijke versie), p. 499. Zie in de context van opsporing en het Wetboek van Strafvordering ook Rb. Den Haag 10 december 2015, ECLI:NL:RBDHA:2015:14365.
41 Zie ook toezichtsrapport nr. 55 (2018).
42 Zie artikel 41 Wiv 2017.
43 Artikel 29 Wiv 2017 en artikel 5 Beleidsregels Wiv 2017. Zie over de inzet van agenten ook, o.a., toezichtsrapport nr. 8a (MIVD, 2006) en 8b (AIVD, 2006) over de inzet van informanten en agenten in het buitenland en toezichtsrapport nr. 37 (2014) over enkele langlopenede agentoperaties door de AIVD.
44 Artikel 41 lid 3 en 6 Wiv 2017.
45 Artikel 41 lid 4 Wiv 2017.
46 *Kamerstukken II* 2016/17, 34588, nr. 3, p. 65.

4. Algemene bepalingen omtrent gegevensverwerking

Dit hoofdstuk zet de algemene bepalingen omtrent gegevensverwerking kort uiteen en past deze toe op het onderwerp automated OSINT. Meer specifiek worden de volgende artikelen uit de Wiv 2017 besproken: 18 (paragraaf 4.1), 19 (paragraaf 4.2), 20 (paragraaf 4.3), 23 (paragraaf 4.4), 24 (paragraaf 4.5) en 60 (paragraaf 4.6).

4.1 Behoorlijke en zorgvuldige gegevensverwerking

Artikel 18 Wiv 2017 schrijft voor dat de verwerking van gegevens slechts plaatsvindt voor zover dat noodzakelijk is voor een goede uitvoering van de Wiv 2017 of de Wet veiligheidsonderzoeken (artikel 18 lid 1 Wiv 2017).[47] Ook moet de gegevensverwerking plaatsvinden in overeenstemming met de Wiv en op 'behoorlijke en zorgvuldige wijze' (artikel 18 lid 2 Wiv 2017). De gegevens moeten zijn voorzien van een aanduiding omtrent de mate van betrouwbaarheid, dan wel een verwijzing naar het document of de bron waaraan de gegevens zijn ontleend (artikel 18 lid 3 Wiv 2017).

De gegevensverwerking die plaatsvindt door het gebruik van een tool bij automated OSINT mag alleen plaatsvinden in het kader van de taakuitvoering van de dienst. Tijdens het openbronnenonderzoek moeten medewerkers een proportionaliteitstoets en subsidiariteitstoets uitvoeren.[48] Dat komt tot uiting in de zoekvragen in het systeem, maar ook in de hoeveelheid gegevens die als resultaat van het onderzoek worden vastgelegd. De resultaten moeten in beginsel zijn voorzien van een verwijzing naar de onderliggende bron en het product waarin de gegevens worden verwerkt krijgt in beginsel een betrouwbaarheidsbeoordeling. Gelet op het gebruik van deze gegevens door de AIVD en de MIVD en de gevolgen die dat kan hebben voor personen waarop die gegevens betrekking hebben, is het van belang dat expliciet wordt vastgesteld wat de kwaliteit van de verzamelde gegevens is.[49]

Als uitwerking van de verplichting tot een 'zorgvuldige gegevensverwerking' dienen de diensten zich ook van tevoren, dus voordat een tool door medewerkers in gebruik wordt genomen en al bij de aanschaf van tools, af te vragen in hoeverre bij de inzet van de tool aan de algemene beginselen omtrent gegevensverwerking wordt voldaan. Zoals in het toezichtsrapport wordt uitgelegd, kunnen bij automated OSINT honderden bronnen tegelijk worden geraadpleegd. Als onderdeel van een zorgvuldige gegevensverwerking dient duidelijk te zijn welke bronnen worden geraadpleegd en uit welke gegevens die bronnen bestaan. Ook de werking van de tools, dat wil zeggen welke functionaliteiten de tool bevat voor de verwerking van gegevens, dient duidelijk te zijn. Deze elementen kunnen van belang zijn voor de beoordeling omtrent het nut van de tool (een element bij het noodzakelijkheidsvereiste), de betrouwbaarheid van de gegevens, maar ook voor de proportionaliteitstoets.

4.2 De verwerking van gevoelige gegevens

Gevoelige gegevens worden in de Wiv 2017 gedefinieerd als gegevens over iemands godsdienst of levensovertuiging, ras, lidmaatschap van een vakvereniging, gezondheid en seksuele leven (artikel 19 Wiv 2017). De verwerking van deze gegevens door de AIVD en de MIVD mag slechts onder strikte voorwaarden plaatsvinden.[50] Dit mag slechts in aanvulling op de verwerking van andere gegevens en voor

47 Zie ook artikel 19 lid 1 en lid 2 Wiv 2017.
48 Zie ook *Kamerstukken II* 2016/17, 34588, nr. 3, p. 32).
49 Zie ook toezichtsrapport nr. 57 (2018) over de gegevensverstrekking door de AIVD binnen Nederland over (vermeende) jihadisten.
50 Artikel 19 lid 3 Wiv 2017. Gegevens over de politieke opvattingen van een persoon worden in de Wiv 2017 niet gezien als gevoelige gegevens, in tegenstelling tot, bijvoorbeeld, artikel 9 lid 1 van de Algemene Verordening Gegevensbescherming.

zover dat voor het doel van de gegevensverwerking onvermijdelijk is (artikel 19 lid 4 Wiv 2017). De term 'onvermijdelijk' geeft aan dat er een zwaardere toets geldt dan bij de eerste aangehaalde algemene noodzakelijkheidstoets uit artikel 18 lid 1 Wiv 2017.[51]

4.3 Verwijdering van gegevens

Gegevens die, gelet op het doel waarvoor zij zijn verwerkt, geen betekenis hebben of hun betekenis hebben verloren moeten worden verwijderd (artikel 20 Wiv 2017). Verwijderen betekent dat de gegevens niet meer toegankelijk zijn voor het reguliere proces (de taakuitvoering van de diensten). Het is mogelijk de gegevens weer toegankelijk te maken als de gegevens weer actueel zijn geworden ten behoeve van de taakuitvoering van de diensten. De verwijderde gegevens worden vernietigd, tenzij wettelijke regels omtrent bewaring daaraan in de weg staan.[52]

Bij automated OSINT worden de gegevens doorgaans verwerkt met algemene bevoegdheden. Dat betekent dat de verwerkte gegevens mogen worden bewaard, totdat deze niet meer van betekenis zijn. In de praktijk zal het daarbij gaan om de bewaring van de resultaten van een zoekslag met de tool(s) voor automated OSINT.

4.4 De zorgplicht voor de geheimhouding van gegevens, bronnen en medewerkers

Het hoofd van de AIVD en het hoofd van de MIVD dragen zorg voor de geheimhouding van de daarvoor in aanmerking komende gegevens, bronnen waaruit de gegevens afkomstig zijn en de veiligheid van de personen met wier medewerking gegevens worden verzameld (artikel 23 Wiv 2017).[53]

Bij automated OSINT vertaalt deze zorgplicht zich met name naar de verplichting zorg te dragen dat niet bekend wordt (buiten de kring van geautoriseerde personen) naar welke personen de diensten onderzoek doen en dat de identiteit van medewerkers die de zoekvragen uitvoeren verborgen blijft. Ook moeten maatregelen worden genomen om verborgen te houden van welke bronnen bij automated OSINT gebruik wordt gemaakt.

4.5 De zorgplicht voor de gegevensverwerking

Het hoofd van de AIVD en het hoofd van de MIVD dragen er tevens zorg voor dat de technische, personele en organisatorische maatregelen worden genomen om de verwerking van gegevens in overeenstemming te laten zijn met hetgeen bij of krachtens de Wiv 2017 is bepaald (artikel 24 Wiv 2017). De hoofden van de diensten hebben aldus een zorgplicht voor de gegevensverwerking. Deze zorgplicht is niet alleen onverkort van toepassing op de concrete inzet van OSINT, maar eveneens op de acquisitie van automated OSINT tools en de - al dan niet via deze tools - toegankelijke bronnen.

Tot de maatregelen die genomen moeten worden in het kader van artikel 24 lid 1 Wiv 2017 behoren in ieder geval: (a) de nodige voorzieningen ter bevordering van de juistheid en volledigheid van de gegevens die worden verwerkt en ter bevordering van de kwaliteit van de gegevensverwerking, (b) de nodige voorzieningen van technische en organisatorische aard ter beveiliging van gegevensverwerking tegen

51 *Kamerstukken II* 2016/17, 34588, nr. 3, p. 34.
52 Artikel 20 lid 3 Wiv 2017.
53 Artikel 23 Wiv 2017.

verlies of aantasting van de gegevens en tegen onbevoegde gegevensverwerking, en (c) de aanwijzing van personen die bij uitsluiting van andere bevoegd zijn tot de verwerking van de gegevens.[54]

Bij automated OSINT vertaalt de zorgplicht zich naar het rekenschap geven van de gegevensverwerkingen en het nemen van technische, personele en organisatorische maatregelen voorafgaand aan het gebruik van de tool.

Als uitwerking van artikel 23 Wiv 2017 dienen technische en organisatorische maatregelen te worden genomen ter beveiliging van de gegevens tegen onbevoegde gegevensverwerking. Deze maatregelen komen ook voorafgaand aan de inzet van de tool tot uiting en krijgen onder andere uitwerking in een autorisatiebeleid.

4.6 Verbod op geautomatiseerde besluitvorming

De AIVD en de MIVD zijn bevoegd om geautomatiseerde data-analyse toe te passen op de gegevens die zij verzamelen (artikel 60 Wiv 2017).[55] Bij de verwerking van gegevens met tools voor automated OSINT kan daarvan sprake zijn, omdat er doorgaans sprake is van bestandsvergelijking.[56]

De toepassing van geautomatiseerde data-analyse is niet aan toestemmingsvereisten verbonden, voor zover het geen betrekking heeft op gegevens uit onderzoeksopdrachtgerichte-interceptie ter identificatie van personen en organisaties betreft.[57] Deze vorm van geautomatiseerde data-analyse is niet aan de orde in dit onderzoek.

Artikel 60 lid 3 Wiv 2017 bevat ten slotte een verbod op het bevorderen of treffen van maatregelen uitsluitend op basis van de resultaten van een geautomatiseerde data-analyse. Daarvoor is menselijke tussenkomst vereist.[58] Het is dus niet toegestaan direct maatregelen te treffen, uitsluitend op basis van een verwerking met een tool voor automated OSINT.

54 Artikel 24 lid 2 Wiv 2017.
55 Meer specifiek: artikel 60 lid 1 sub d Wiv 2017.
56 Artikel 60 lid 2 sub a Wiv 2017.
57 Artikel 50 lid 1 sub b jo lid 4 jo artikel 60 Wiv 2017.
58 Artikel 60 lid 3 Wiv 2017.

5. Overzicht wettelijke vereisten

De CTIVD komt in ieder geval tot de volgende vereisten voor het gebruik van tools voor automated OSINT:

- De gegevensverwerking moet een bepaald doel treffen, noodzakelijk zijn en op behoorlijke en zorgvuldige wijze plaatsvinden. De gegevens moeten bovendien zijn voorzien van een aanduiding omtrent de mate van betrouwbaarheid, dan wel een verwijzing naar het document of de bron waaraan de gegevens zijn ontleend (artikel 18 Wiv 2017).
- De verwerking van gevoelige gegevens mag enkel plaatsvinden in aanvulling op de verwerking van andere gegevens en voor zover dat onvermijdelijk is voor de taakuitvoering van de diensten (artikel 19 Wiv 2017).
- De overgenomen publiek toegankelijke gegevens moeten worden verwijderd als deze niet meer van betekenis zijn (artikel 20 Wiv 2017).
- Als voorafgaand redelijkerwijs kan worden overzien dat stelselmatig persoonsgegevens worden overgenomen uit voor een ieder toegankelijke informatiebronnen, moet een aanvraag worden gedaan voor de inzet van de algemene bevoegdheid op basis van artikel 38 Wiv 2017.
- Als het verzamelen van gegevens omtrent een persoon uit een voor een ieder toegankelijke informatiebron toekomstgericht is, moet een aanvraag worden gedaan voor de inzet van de bevoegdheid tot observatie voor een periode van maximaal drie maanden (artikel 40 Wiv 2017).
- Het is niet toegestaan direct maatregelen te treffen uitsluitend op basis van een verwerking met een tool voor automated OSINT. Daarvoor is menselijke tussenkomst vereist (artikel 60 Wiv 2017).
- De hoofden van de diensten dragen zorg voor de geheimhouding van de daarvoor in aanmerking komende gegevens, de daarvoor in aanmerking komende bronnen waaruit de gegevens afkomstig zijn en de veiligheid van de personen met wier medewerking gegevens worden verzameld (artikel 23 Wiv 2017).
- De hoofden van de diensten dragen er zorg voor dat de technische, personele en organisatorische maatregelen in verband met de verwerking van gegevens in overeenstemming is met de wet (artikel 24 Wiv 2017). Tot de maatregelen behoren in ieder geval (a) de nodige voorzieningen ter bevordering van de juistheid en volledigheid van de gegevens die worden verwerkt en ter bevordering van de kwaliteit van de gegevensverwerking, (b) de nodige voorzieningen van technische en organisatorische aard ter beveiliging van gegevensverwerking tegen verlies of aantasting van de gegevens en tegen onbevoegde gegevensverwerking, en (c) de aanwijzing van personen die bij uitsluiting van anderen bevoegd zijn tot de verwerking van de gegevens.

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

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