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

TOEZICHTSRAPPORT

Automated OSINT: tools en bronnen voor openbronnenonderzoek

Inhoudsopgave

Commissie van Toezicht
op de Inlichtingen- en
Veiligheidsdiensten

CTIVD nr. 74

TOEZICHTSRAPPORT

Automated OSINT: tools en bronnen voor openbronnenonderzoek

Samenvatting

De Wet op de inlichtingen- en veiligheidsdiensten (Wiv 2017) biedt de AIVD en de MIVD de mogelijkheid om publiek toegankelijke (persoons)gegevens te verzamelen en te verwerken. Dit wordt ook wel openbronnenonderzoek genoemd of aangeduid met de term OSINT ('open source intelligence'). OSINT wordt door de wetgever niet als een indringend inlichtingenmiddel gezien. Het betreft een algemene bevoegdheid van de diensten, waarbij er een onderscheid is tussen een niet-stelselmatige en stelselmatige inzet. Voor het stelselmatig verzamelen van persoonsgegevens uit voor een ieder toegankelijke informatiebronnen is toestemming vereist.

Wanneer openbronnenonderzoek geautomatiseerd plaatsvindt met behulp van specialistische software of webapplicaties, is er sprake van 'automated OSINT'. In dit onderzoek worden daarbij twee elementen onderscheiden: de *tools* die worden gebruikt en de *bronnen* (datasets) die via deze tools geraadpleegd kunnen worden. Bij de 'tools' gaat het om software met zoekfuncties en netwerkanalysefuncties, waarbij een grote diversiteit aan bronnen kan worden bevraagd. Deze tools kunnen afkomstig zijn van commerciële aanbieders of door de diensten zelf zijn ontwikkeld.

Tools voor automated OSINT bieden twee grote voordelen ten opzichte van regulier openbronnen-onderzoek via een webbrowser. Het eerste grote voordeel is het gebruiksgemak; in één zoekslag met een tool voor automated OSINT kunnen tot wel honderden bronnen tegelijkertijd worden bevraagd. De resultaten kunnen vervolgens door de tools worden gevisualiseerd. Het tweede grote voordeel dat het gebruik van de tools voor de diensten oplevert is dat bronnen kunnen worden geraadpleegd die op commerciële basis op een gebruikersvriendelijke manier door de leverancier worden aangeboden. Een voorbeeld daarvan betreffen gelekte gegevens van gebruikers van sociale mediadiensten. Leveranciers kunnen deze datasets samenvoegen als één raadpleegbare bron (een 'samengestelde dataset') met soms wel miljarden gegevens.

Een voorbeeld van commerciële gegevens die via deze tools kunnen worden geraadpleegd, betreffen locatiegegevens die worden gegenereerd door advertenties die worden getoond aan gebruikers van applicaties. De aanbieders van commerciële tools voor OSINT kunnen advertentiegegevens afnemen bij datahandelaren ('data brokers') en deze via hun tool beschikbaar stellen aan klanten, waaronder inlichtingen- en veiligheidsdiensten.

De omvang, aard en diversiteit aan persoonsgegevens in deze automated OSINT tools kan een ernstiger inbreuk op fundamentele rechten met zich meebrengen, in het bijzonder op het recht op privacy, dan het raadplegen van gegevens in voor een ieder toegankelijke informatiebronnen op internet, zoals gegevens via een zoekmachine of publiek toegankelijke gegevens op sociale media.

Uit de memorie van toelichting van de Wiv 2017 kan worden opgemaakt dat destijds geen rekening is gehouden met deze automated OSINT-praktijk, die zich in de nabije toekomst verder zal blijven ontwikkelen. OSINT is nadrukkelijk niet meer alleen het 'naslaan' van telefoonboeken of zoeken van gegevens op internet met een zoekmachine. Het onderhavige onderzoek weerspiegelt het volgende: met automated OSINT kunnen honderden bronnen van diverse herkomst tegelijkertijd worden geraadpleegd, waaronder locatiegegevens of gegevens uit gelekte datasets. De huidige praktijk van automated OSINT brengt een ernstiger privacy-inbreuk met zich mee dan destijds is voorzien.

Deze bevinding leidt tot aanbeveling 1:
Gezien de aard, diversiteit en hoeveelheid van de in het geding zijnde gegevens beveelt de CTIVD de wetgever aan een meer voorzienbare wettelijke grondslag met voldoende waarborgen te creëren ten aanzien van automated OSINT, zowel voor wat betreft de tools als de via deze tools te raadplegen bronnen.

De rechtmatigheidstoets van de CTIVD richt zich in dit onderzoek primair op de OSINT-tools en de via deze tools te raadplegen datasets (de bronnen). Hoe deze tools en bronnen in concrete gevallen worden ingezet is geen onderdeel van het onderzoek. De CTIVD vindt het essentieel dat de diensten voorafgaand aan de concrete inzet weten hoe de tools werken en welke bronnen daarbij kunnen worden geraadpleegd. Alleen met deze kennis kan een gedegen toets worden uitgevoerd om te bepalen hoe de verwerking van deze gegevens met deze tools zich verhoudt tot de algemene bepalingen omtrent gegevensverwerking uit de Wiv 2017. Deze bepalingen schrijven onder andere voor dat de verwerking van gegevens door de diensten proportioneel dient te zijn. Daarmee wordt bedoeld dat er een juiste balans moet zijn tussen het belang de gegevens te verwerken voor het betreffende inlichtingenonderzoek en de ernst van de inbreuk op de fundamentele rechten van de betrokkene.

De CTIVD beoogt met dit onderzoek de volgende onderzoeksvraag te beantwoorden:
Hebben de AIVD en de MIVD de werking van de tools voor automated OSINT en de herkomst en de aard van de achterliggende bronnen in voldoende mate doorgrond met het oog op de naleving van de bepalingen omtrent gegevensverwerking?

Het antwoord op de onderzoeksvraag luidt dat de AIVD en MIVD de werking (de functionaliteiten) van de tools voor automated OSINT en de herkomst en de aard van de via deze tools te raadplegen bronnen in onvoldoende mate hebben doorgrond om zodoende aan de bepalingen in de Wiv 2017 met betrekking tot gegevensverwerking te kunnen voldoen. De CTIVD stelt vast dat meerdere verbeteringen noodzakelijk zijn om automated OSINT in overeenstemming met de wet te brengen. De diensten dienen (alsnog) de werkwijzen en (zo goed als mogelijk) de achterliggende bronnen van de tools in kaart brengen en daarop mitigerende maatregelen nemen om onrechtmatigheden in de toekomst te voorkomen.

Deze bevinding leiden tot aanbeveling 2:
De AIVD en de MIVD dienen zich bij de selectie en verwerving van tools voor automated OSINT (en daarmee ook de achterliggende bronnen) ook te richten op het waarborgen van een zorgvuldige gegevensverwerking. Het verdient de voorkeur dat de diensten in gezamenlijkheid een beleidskader ontwikkelen met bijbehorende werkinstructies.

In het belang van rechtszekerheid, de rechtmatigheid en de slagkracht van de diensten (vanwege de continuïteit van de rechtmatige gegevensverwerking bij OSINT) zal de CTIVD, in dialoog met de diensten, inzetten op de totstandkoming van een werkbaar tijdelijk toetsingskader dat door de diensten wordt vertaald in beleid, procedures en werkinstructies. In dit tijdelijke toetsingskader moet onder meer aandacht zijn voor de inrichting van een voorafgaande toets op de bepalingen omtrent gegevensverwerking, het criterium van stelselmatigheid bij openbronnenonderzoek en de omgang met bronnen waarvan de herkomst en juistheid van de gegevens niet goed is vast te stellen.

OSINT vindt niet exclusief plaats binnen het domein van de inlichtingen- en veiligheidsdiensten, maar ook elders in het nationale veiligheidsdomein (bijvoorbeeld bij de NCTV) en daarbuiten (onder meer bij andere overheden). Dit rapport stelt vast dat OSINT zich in de loop der jaren verder heeft ontwikkeld en dat daarbij tools kunnen worden gebruikt die tegelijkertijd honderden bronnen raadplegen. De resultaten daarvan kunnen snel, overzichtelijk en in onderlinge samenhang worden weergegeven. Deze achterliggende bronnen kunnen locatiegegevens of gelekte gegevens bevatten. De verwerking van deze gegevens maakt een verdergaande inbreuk op de fundamentele rechten van betrokkenen dan bij OSINT via reguliere zoekmachines of op sociale mediadiensten.

De CTIVD verzoekt derhalve de ministers van Binnenlandse Zaken en Koninkrijksrelaties en van Defensie om dit rapport ook elders binnen de overheid onder de aandacht te brengen en bij toezending het Parlement te verzoeken het tevens ter kennis te brengen bij de Vaste Commissie voor Digitale Zaken van de Tweede Kamer.

CTIVD nr. 74

TOEZICHTSRAPPORT

Automated OSINT: tools en bronnen voor openbronnenonderzoek

1. Inleiding

Dit toezichtsrapport gaat over 'automated open source intelligence' (hierna: automated OSINT). OSINT wordt in dit rapport ook aangeduid met de term 'openbronnenonderzoek' en de in de Wiv 2017 gehanteerde term 'het verzamelen van gegevens uit voor een ieder toegankelijke informatiebronnen'. Automated OSINT wordt uitgevoerd met behulp van 'tools', zoals software of webapplicaties. De tools kunnen afkomstig zijn van commerciële aanbieders of zelf zijn ontwikkeld door de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) en de Militaire Inlichtingen- en Veiligheidsdienst (MIVD).

De tools voor automated OSINT die in dit onderzoek centraal staan, bevatten zoek- en analysefuncties met toegang tot een grote diversiteit aan bronnen, zoals artikelen op nieuwswebsites en publiek toegankelijke gegevens op sociale mediadiensten. Het is ook mogelijk persoonsgegevens via deze tools te raadplegen die door een commerciële dienstverlener zijn verzameld en voorbewerkt. Deze 'samengestelde datasets' kunnen ook gelekte persoonsgegevens van gebruikers van sociale mediadiensten bevatten. Ook bieden deze tools de mogelijkheid commercieel beschikbare gegevens te raadplegen, zoals een dataset met locatiegegevens.

Medewerkers van de AIVD en de MIVD met toegang tot de tools kunnen een zoekvraag invoeren in de tool, zoals de vraag of aan een target (een persoon die onder de aandacht staat van de diensten) een profiel van een sociale mediadienst is te koppelen en daarmee persoonsgegevens over dit target verzamelen. Dit wordt 'targetgericht onderzoek' genoemd. Het is ook mogelijk met de tools 'fenomeenonderzoek' uit te voeren, dat met name ziet op het in kaart brengen van sociaal-maatschappelijke ontwikkelingen en het identificeren van trends. Het kan dan bijvoorbeeld gaan om het verzamelen en analyseren van informatie uit nieuwsartikelen om een normbeeld voor een bepaalde regio of over een bepaald thema vast te stellen (daarbij kunnen ook persoonsgegevens worden verwerkt). Aangezien bij targetgericht onderzoek met behulp van tools voor automated OSINT doorgaans een grotere privacy-inbreuk plaatsvindt dan bij fenomeenonderzoek, richt dit onderzoek zich met name op targetgericht onderzoek.

Wettelijke regeling

De Wet op de inlichtingen- en veiligheidsdiensten (Wiv 2017) biedt de AIVD en de MIVD in artikel 25 Wiv 2017 de bevoegdheid gegevens uit voor een ieder toegankelijke informatiebronnen te verzamelen. Op grond van artikel 38 Wiv 2017 zijn de diensten ook bevoegd tot het *stelselmatig* verzamelen van gegevens omtrent personen uit voor een ieder toegankelijke informatiebronnen, al dan niet met een technisch hulpmiddel. Bij stelselmatigheid moet een aanvraag voor de inzet van de bevoegdheid worden gedaan en toestemming worden verkregen.[1]

1 Zie ook het toetsingskader bij dit rapport (Bijlage I).

Het onderscheid tussen openbronnenonderzoek en stelselmatig openbronnenonderzoek is door de wetgever in de Wiv 2017 gemaakt naar aanleiding van de 'Privacy Impact Assessment Wiv 20XX'. In dit rapport werd duidelijk gemaakt dat bij stelselmatig openbronnenonderzoek naar een persoon zich een meer ernstige privacy-inbreuk kan voordoen.[2] Er is sprake van stelselmatigheid als het op voorhand redelijkerwijs voorzienbaar is dat een 'min of meer volledig beeld van bepaalde aspecten uit het privéleven van een persoon' zal worden verkregen.

De diensten dienen bij de verwerking van gegevens te voldoen aan de algemene bepalingen omtrent gegevensverwerking uit de WIv 2017. Deze bepalingen schrijven onder andere voor dat de verwerking van gegevens plaatsvindt voor de taakuitvoering van de diensten, dat deze proportioneel is en dat het hoofd van de dienst zorg draagt voor het nemen van maatregelen ter bevordering van de juistheid en volledigheid van de gegevens die worden verwerkt en ter bevordering van de kwaliteit van de gegevensverwerking.[3] Het wettelijk kader is nader toegelicht in het toetsingskader (Bijlage I).

Maatschappelijke discussie

De maatschappelijke impact van openbronnenonderzoek binnen het nationale veiligheidsdomein is in 2021 nog eens duidelijk geworden door de discussie over het gebruik van nepprofielen op sociale mediadiensten door de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV).[4] Ook in het buitenland is er toenemende aandacht voor OSINT. Zo leidde in de Verenigde Staten het gebruik van onder andere de tool 'Locate X' door Amerikaanse overheidsdiensten tot vragen van Amerikaanse senatoren en tot een (thans lopend) onderzoek van de 'Office of Inspector General' van het 'Department of Homeland Security'.[5] Verder loopt in de Verenigde Staten bij de onafhankelijke toezichthouder 'Privacy and Civil Liberties Oversight Board' (PCLOB) een onderzoek naar "FBI Collection of Open Source Data".[6] In de Verenigde Staten richt de discussie zich met name op de vraag of een rechterlijke machtiging ('warrant') noodzakelijk is bij het opvragen van locatiegegevens met dergelijke tools.

Buiten het nationale veiligheidsdomein staan de implicaties van openbronnenonderzoek eveneens in de belangstelling.[7] Zo is er een wetsvoorstel in voorbereiding waarin een identieke bevoegdheid voor het stelselmatig overnemen van persoonsgegevens uit publiek toegankelijke informatiebronnen wordt geregeld binnen het opsporingsdomein.[8]

Reikwijdte onderzoek en onderzoeksvraag

De rechtmatigheidstoets van de CTIVD richt zich in dit onderzoek primair op OSINT-tools en de via deze tools te raadplegen gegevens (de bronnen). Hoe deze tools en bronnen in concrete gevallen worden ingezet en de vraag of deze inzet stelselmatig is, is geen onderdeel van het onderzoek. In dit onderzoek is nagegaan of in het kader van een zorgvuldige gegevensverwerking van tevoren is nagedacht over de naleving van de algemene bepalingen omtrent gegevensverwerking in de Wiv 2017. Daarbij gaat het in de eerste plaats om de tools zelf: hoe zijn deze geselecteerd, hoe werken ze en hoe zijn daarbij

2 B.J. Koops e.a., 'Privacy Impact Assessment Wet op de Inlichtingen- en veiligheidsdiensten 20XX', TNO/PILab/Tilburg University 2016. *Kamerstukken II* 2016/17, 34588, nr. 3, p. 63 en *Kamerstukken II* 2016/17, 34588, nr. 18, p. 53.
3 Respectievelijk artikel 18 en artikel 24 Wiv 2017.
4 Zie A. Kouwenhoven, E. Rosenberg & R. van der Poel, 'NCTV volgt heimelijk burgers op sociale media', *NRC*, 9 april 2021 en A. Kouwenhoven, E. Rosenberg & R. van der Poel, 'Linkse activist werd jaren online gevolgd door de NCTV', *NRC*, 23 juli 2021.
5 'DHS Use of Cell-Phone Surveillance Devices', *Office of Inspector General, U.S. Department of Homeland Security*, beschikbaar op www.oig.dhs.gov/node/6227. Zie tevens, o.a, B. Tau, 'U.S. Government Contractor Embedded Software in Apps to Track Phones', *The Wall Street Journal*, 7 augustus 2020, J. Cox, 'Secret Service Bought Phone Location Data from Apps, Contract Confirms', *Vice*.com, 17 augustus 2020, 'How the U.S. Military Buys Location Data from Ordinary Apps', *Vice*.com 16 november 2020 en C. Savage, 'Intelligence Analysts Use U.S. Smartphone Location Data Without Warrants, Memo Says', *The New York Times*, 22 januari 2021.
6 'FBI Collection of Open-Source Data', *U.S. Privacy and Civil Liberties Oversight Board*. Beschikbaar op www.pclob.gov/projects.
7 Zie, o.a., H. von Piekartz, 'Gemeenten kijken op grote schaal en in het geheim mee met burgers op sociale media', *De Volkskrant*, 18 mei 2021 en E. Rosenberg & K. Berkhout, 'Leger verzamelde data in Nederland', *NRC*, 15 november 2020.
8 Wetsvoorstel tot vaststelling van het nieuwe Wetboek van Strafvordering, juli 2020 (ambtelijke versie).

de algemene vereisten voor gegevensverwerking in acht genomen? In de tweede plaats richt het onderzoek zich op de bronnen die via deze tools worden geraadpleegd: welke bronnen betreft het en hoe verhouden deze zich tot de algemene bepalingen over gegevensverwerking?

Daarmee beoogt de CTIVD de volgende onderzoeksvraag te beantwoorden:
Hebben de AIVD en de MIVD de werking van de tools voor automated OSINT en de herkomst en de aard van de achterliggende bronnen in voldoende mate doorgrond met het oog op de naleving van de bepalingen omtrent gegevensverwerking?

De door de CTIVD gekozen onderzoeksperiode bestrijkt de periode van 1 juli 2020 tot en met 31 maart 2021. De diensten hebben desgevraagd aangegeven dat deze periode representatief is.

De keuze voor het beperken van dit onderzoek tot de voorfase is gelegen in het feit dat tijdens het verkennend onderzoek bleek dat de diensten voorafgaand aan en tijdens het verwervingsproces van een tool weinig aandacht hadden besteed aan de naleving van de algemene vereisten voor gegevensverwerking bij automated OSINT. De kans is daardoor groot dat zich onrechtmatigheden voordoen bij de inzet van tools voor automated OSINT voor de verzameling en verdere verwerking van gegevens. Ook bleek dat openbronnenonderzoek op basis van de algemene bevoegdheid in artikel 25 Wiv 2017 door de diensten niet altijd te worden gelogd of vastgelegd als het geen resultaten opleverde. Toezicht op de naleving van artikel 25 Wiv 2017 in verhouding tot artikel 38 Wiv 2017 (het stelselmatig verzamelen van gegevens omtrent een persoon uit voor een ieder toegankelijke informatiebronnen) is daardoor niet goed mogelijk.

De CTIVD acht het essentieel dat de diensten het proces van automated OSINT inrichten zodat deze in overeenstemming is met de Wiv 2017. Hiervoor is het nodig dat de diensten voldoende zicht krijgen op de werking van de tools, zoals de functionaliteiten die de tools bieden en de achterliggende bronnen. Met deze kennis kunnen zij bezien hoe de tools en bronnen zich verhouden tot de wettelijke vereisten voor gegevensverwerking en de wettelijke bevoegdheid openbronnenonderzoek uit te voeren (al dan niet stelselmatig).

De achterliggende gegevens die via tools voor automated OSINT raadpleegbaar zijn kunnen het karakter hebben van een bulkdataset. Dit aspect is als zodanig geen onderwerp van dit onderzoek, maar is onder meer eerder aan bod gekomen in de CTIVD-rapporten 55 (over door verwerving van door derden op internet aangeboden bulkdatasets), 70 (verzamelen van bulkdatasets met de hackbevoegdheid en de verdere verwerking daarvan) en 71 (verzamelen en verder verwerken van passagiersgegevens van luchtvaartmaatschappijen).

Methodiek

De tools voor automated OSINT en de achterliggende bronnen worden aan de hand van het toetsingskader (Bijlage I) op rechtmatigheid getoetst. Bij het oordeel 'onrechtmatig' is sprake van strijdigheid met wet- of regelgeving. Deze wet- en regelgeving bestaat uit de Wiv 2017, jurisprudentie, en door de betreffende ministers overgenomen aanbevelingen uit eerdere toezichtsrapporten van de CTIVD. Indien de werkwijze, beleid of processen van een dienst gebreken vertonen, wordt dit in het rapport een onzorgvuldigheid genoemd.

Gedurende het onderzoek zijn gesprekken gevoerd met medewerkers van verschillende teams bij beide diensten. Ook zijn interne stukken bij de AIVD en de MIVD bestudeerd, zoals beleid en werkinstructies met betrekking tot openbronnenonderzoek en werkdocumenten met betrekking tot de gebruikte tools voor automated OSINT. Voor het benodigde inzicht zijn verder literatuur en commerciële (OSINT-) producten bestudeerd. De diensten hebben bevestigd dat zij alle voor het beantwoorden van de onderzoeksvraag relevante informatie hebben overgelegd.

Geheime bijlage

Dit rapport heeft een geheime bijlage. In deze bijlage staan geen onrechtmatigheden die niet in het openbare rapport zijn beschreven. De geheime bijlage bevat meer gedetailleerde informatie die inzicht geeft in de werkwijze van de diensten met betrekking tot automated OSINT en is om deze reden als 'geheim' gerubriceerd.

Leeswijzer

Het rapport is als volgt opgebouwd. Hoofdstuk 2 schetst op hoofdlijnen de verschillende manieren waarop (automated) OSINT in het algemeen en binnen de AIVD en de MIVD plaatsvindt. Hoofdstuk 3 geeft de bevindingen weer over de naleving van wettelijke vereisten voor gegevensverwerking in de praktijk van automated OSINT bij de AIVD en de MIVD. Het rapport sluit af met hoofdstuk 4 waarin de conclusies en aanbevelingen staan beschreven. Het rapport kent drie bijlagen: een geheime bijlage, een toetsingskader (Bijlage I) en een begrippenlijst (Bijlage II).

2. Automated OSINT: Voorbeelden van tools en bronnen

OSINT kan op veel verschillende manieren plaatsvinden en het domein van OSINT heeft zich in de afgelopen jaren ontwikkeld tot een technisch hoogwaardige inlichtingenmethode. Het is echter van belang voor de rest van het rapport te realiseren dat – vergeleken met de situatie in 2014 toen de CTIVD een onderzoek verrichtte naar het verzamelen van gegevens van sociale mediadiensten door de AIVD[9] – er anno 2021 aanzienlijk meer mogelijkheden zijn om gegevens te verzamelen én te verwerken met specialistische tools. Met deze specialistische tools kunnen de diensten verschillende sociale mediadiensten (zoals 'Facebook' en 'Twitter') tegelijk raadplegen, maar kan ook gebruik worden gemaakt van grote hoeveelheden commercieel beschikbaar gestelde gegevens. De memorie van toelichting van de Wiv 2017 spreekt niet van deze ontwikkeling op het gebied van OSINT, waardoor het voor burgers onvoldoende duidelijk is in welke mate een inbreuk op fundamentale rechten kan plaatsvinden als gevolg van deze ontwikkelingen in het domein van OSINT.

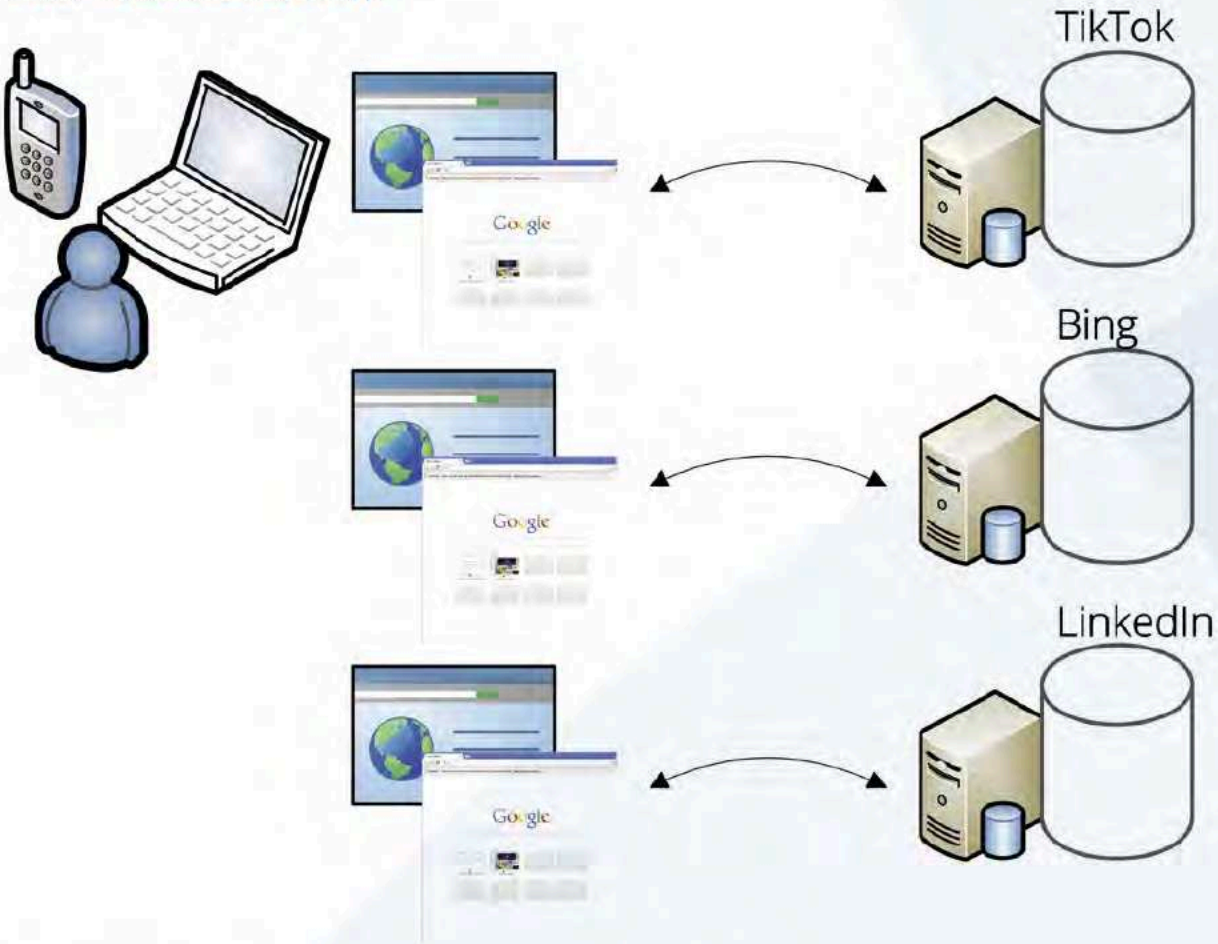
Dit hoofdstuk legt uit hoe OSINT en automated OSINT in het algemeen in zijn werk gaat en hoe tools voor automated OSINT bij de AIVD en de MIVD worden toegepast. Eerst wordt ingegaan op de diverse vormen van OSINT (waaronder het gebruik van 'tools') en vervolgens op de bronnen die daarbij kunnen worden geraadpleegd (paragrafen 2.1 en 2.2). Paragraaf 2.3 beschrijft de ontwikkeling van gespecialiseerde tools en commercieel aangeboden bronnen. De praktijk van de AIVD en MIVD met betrekking tot automated OSINT komt aan bod in de paragrafen 2.4 tot en met 2.7.

2.1 Vormen van OSINT

Deze paragraaf biedt inzicht in de ontwikkeling op het gebied van (automated) OSINT. OSINT kan in drie categorieën worden onderverdeeld, namelijk raadpleging (1) via een webbrowser of app, (2) via een 'Application Programming Interface' (API) en (3) door gebruik te maken van een gespecialiseerde applicatie ('tool').

9 Toezichtsrapport nr. 39 (2014) inzake onderzoek door de AIVD op sociale media.

OSINT via webbrowser of app

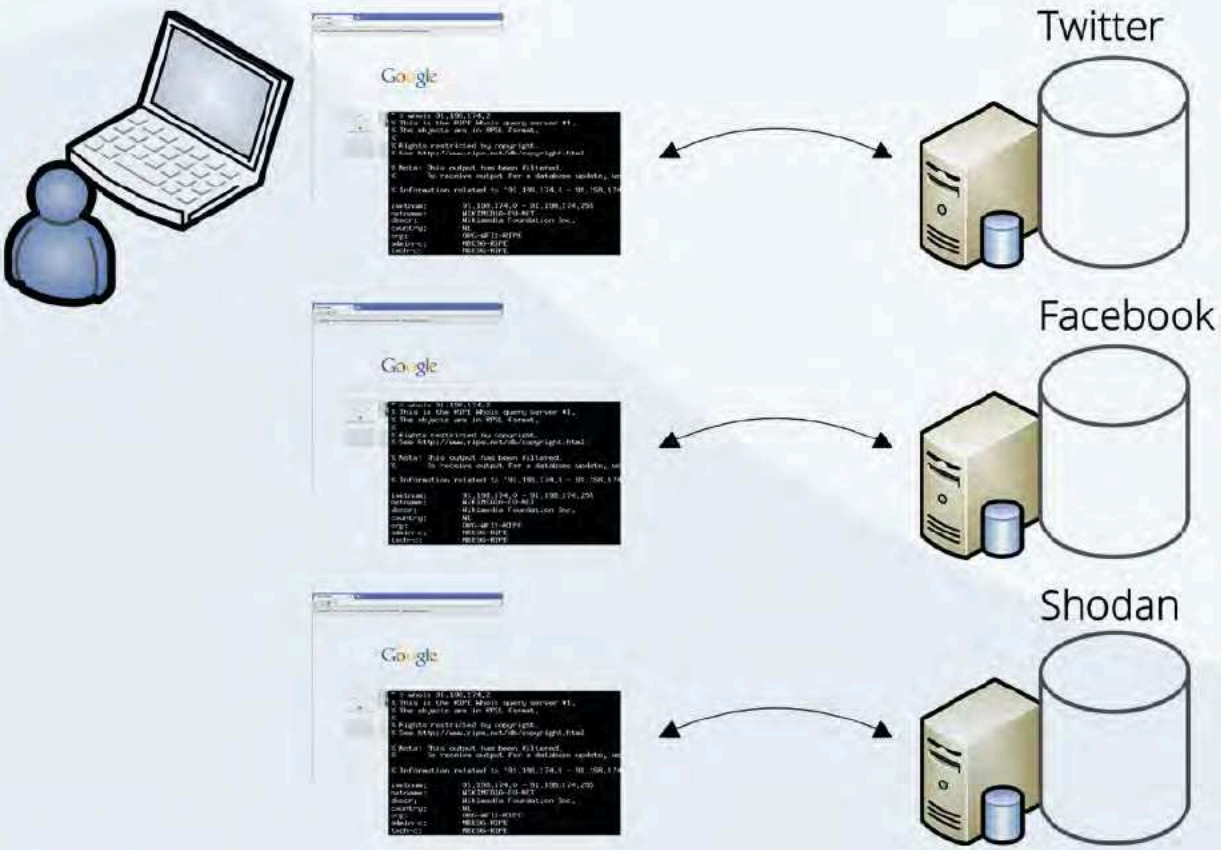


Figuur 2.1: OSINT via de webbrowser met enkele voorbeeldbronnen.

Een ieder is bekend met het gebruik van zoekmachines (zoals 'Google') of het bekijken van een profiel op een sociale mediadienst (zoals 'Facebook' of 'Linkedin') door middel van een webbrowser (zoals 'Google Chrome', 'Firefox' of 'Microsoft Edge') op een laptop of een app op een mobiele telefoon.

Zoekmachines indexeren, over het algemeen, webpagina's die beschikbaar zijn op het internet. Met zogenaamde 'crawlers' worden die verzameld, geïndexeerd en opgeslagen in een database. Deze database is te bevragen door een zoekmachine zoals Google. Andere bekende zoekmachines zijn 'Bing', 'Baidu' en 'Yandex'. Buiten de voor de hand liggende zoekmachines bestaat bijvoorbeeld ook 'The Wayback Machine'; een digitaal archief van het wereldwijde web.[10] Apps bieden vaak toegang tot een specifiek platform, hebben een zelfstandige functie of zijn een aanvulling op zoekmachines.

10 Zie o.a., H. Gibson, 'Acquisition and Preparation of Data for OSINT Investigations', in: B. Akhgar, S. Bayerl & F. Sampson, *Open Source Intelligence Investigation*, Springer: 2016.

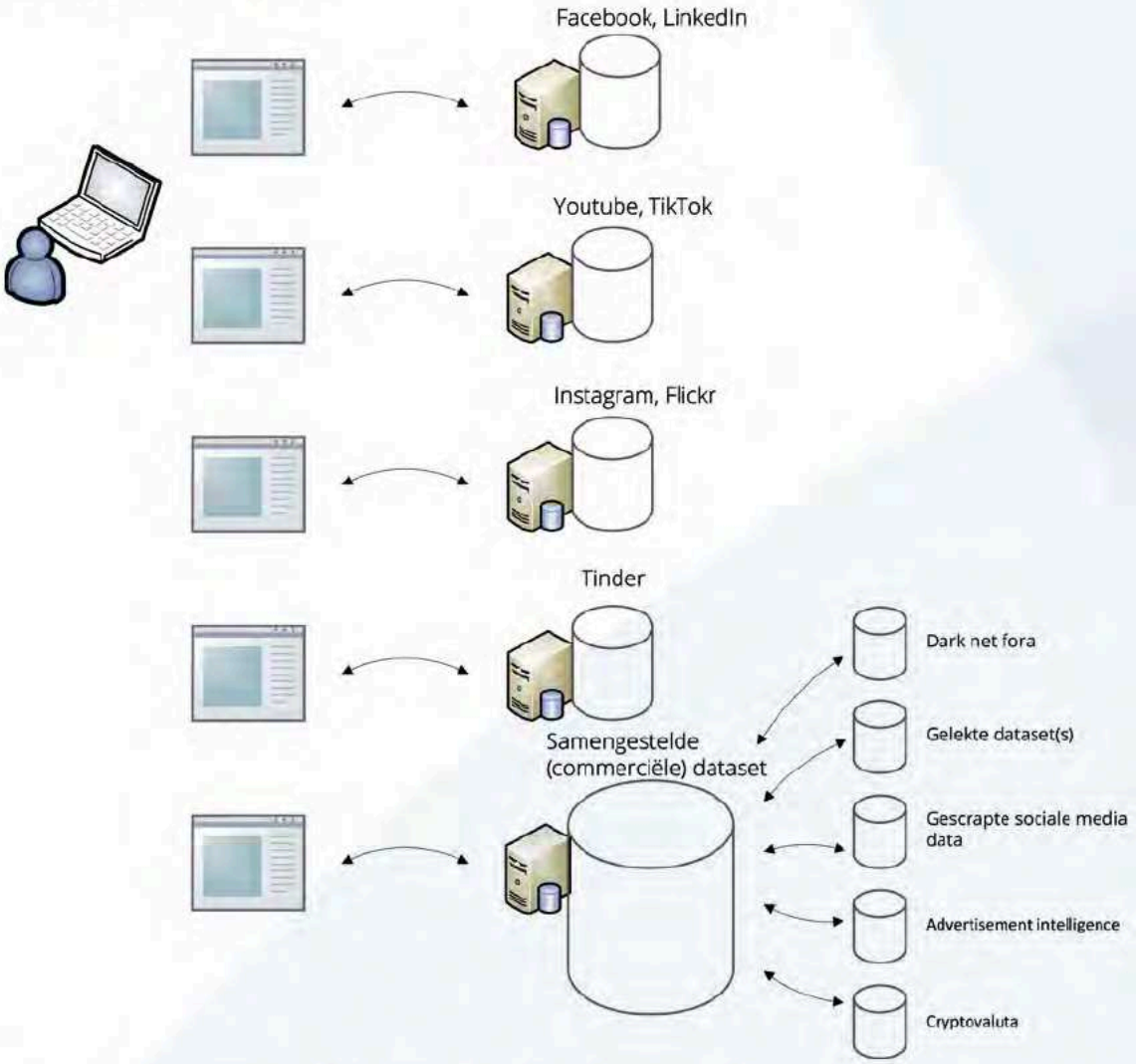


Figuur 2.2: OSINT via API met enkele voorbeeldbronnen.

Een Application Programming Interface (API) is een verzamelnaam voor een computerprogramma dat communiceert met een ander programma (oftewel 'backend'), zodat er gegevensuitwisseling kan plaatsvinden. Een voorbeeld van een API is de functionaliteit die veel websites aanbieden voor een mogelijkheid om op hun platform in te loggen middels een sociale media-account, zoals van Facebook, LinkedIn of Google.

De API voorziet de website van identificatie-informatie, waarmee de gebruiker op het achterliggende sociale mediaplatform wordt geauthenticeerd. Soms is het daarbij noodzakelijk dat een account wordt aangemaakt voor het benaderen van de API. Het voordeel van het raadplegen van gegevens via een API, ten opzichte van het bezoeken van een webpagina via een browser, is dat gestructureerde data beter kan worden opgehaald zonder overbodige 'overhead-informatie', zoals de opmaak van de webpagina. Een ander belangrijk verschil is dat het bevragen van een API eenvoudiger te automatiseren is. Dit maakt het openbronnenonderzoek efficiënter in vergelijking met een webbrowser.

Tools voor automated OSINT



Figuur 2.3: (Automated) OSINT via tools met enkele voorbeeldbronnen.

Tools voor automated OSINT combineren het uitvoeren van OSINT via de webbrowser, het verwerken van gegevens via de API van websites en het verwerken van gegevens in samengestelde (commerciële) datasets. Met behulp van een zoekcriterium, zoals de naam van een persoon of een telefoonnummer, kunnen in dat geval in één keer alle beschikbare gegevens in bovengenoemde bronnen tegelijkertijd worden geraadpleegd. De resultaten worden vervolgens aan de gebruiker van de tool, al dan niet in onderlinge relatie, ter beschikking worden gesteld. Op deze wijze kan op een efficiënte manier een grote hoeveelheid databronnen worden geraadpleegd, om zo een beeld te krijgen van de beschikbare gegevens over een persoon.[11] Het raadplegen van dezelfde gegevens in verschillende bronnen kan bijdragen aan de juistheid en betrouwbaarheid van het gegeven. De gegevens die van belang zijn voor het onderzoek worden vervolgens overgenomen en verder verwerkt ten behoeve van de taakuitvoering.

De methoden voor de analyse van gegevens met behulp van dit soort tools, worden in de literatuur opgedeeld in drie categorieën, te weten lexicale analyse, netwerkanalyse en georuimtelijke analyse, dan wel een combinatie van deze drie varianten.[12] Bij lexicale analyse gaat het om het bijeenbrengen van (grote hoeveelheden) tekst. De tools maken het ook mogelijk om netwerkanalyses uit te voeren en

11 Zie o.a., H. Gibson, 'Acquisition and Preparation of Data for OSINT Investigations', in: B. Akhgar, S. Bayerl & F. Sampson, *Open Source Intelligence Investigation*, Springer: 2016.
12 H. Williams en I. Blum, *Defining Second Generation Open Source Intelligence (OSINT) for the Defense Enterprise*, RAND: 2018, p. 23.

deze te visualiseren, waardoor bijvoorbeeld relaties tussen personen of entiteiten duidelijk worden. Georuimtelijke analyse tot slot wordt bijvoorbeeld toegepast om bepaalde gegevens aan een specifieke locatie te koppelen (dit wordt ook wel 'geotagging' genoemd). De tools die beschikbaar zijn, maken het vervolgens mogelijk deze data te visualiseren en analyseren. Daarmee is het bijvoorbeeld ook mogelijk verplaatsingen van personen en objecten zichtbaar te maken.

2.2 Ontwikkeling in OSINT

Traditioneel wordt bij OSINT vaak verwezen naar informatie die afkomstig is uit telefoonboeken, kranten, tijdschriften, (nieuws)websites, analyses van denktanks of (wetenschappelijke) artikelen. Deze bronnen betreffen voornamelijk statische content, gepubliceerd door organisaties, persbureaus, overheden en individuen.

Ook gegevens op het 'deep web' of 'dark web', zoals online forums of darknet markets, kunnen voor een ieder toegankelijke informatie betreffen. Het deep web is 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. Het dark web bestaat uit het gedeelte van het internet waar de IP-adressen van genetwerkte computers verborgen zijn door middel van speciale software, zoals 'The Onion Router' (Tor).

Vandaag de dag speelt 'user generated content' (informatie die door gebruikers van een bepaald medium wordt aangeleverd, in het bijzonder sociale media), een belangrijke rol bij het vinden van persoonsgerelateerde informatie.[13] Hierbij kan onder meer gedacht worden aan het delen van berichten (zoals op Facebook en LinkedIn), het delen van video's (zoals op 'YouTube' en 'TikTok') en het delen van foto's (zoals op 'Instagram' en 'Flickr'). Daarnaast bestaat er een levendige handel in de gegevens van personen over het bezoeken van websites en activiteiten op sociale mediadiensten. Gegevens uit advertenties, maar ook uit cookies, worden door vele partijen verhandeld en kunnen (uiteindelijk ook) via een bedrijf die tools voor automated OSINT aanbiedt terechtkomen bij andere partijen, zoals inlichtingen- en veiligheidsdiensten.

2.3 Gespecialiseerde tools en commercieel beschikbare bronnen

In toenemende mate is er sprake van het commercieel beschikbaar stellen of toegankelijk maken van bronnen, al dan niet via gespecialiseerde tools. Er zijn diensten op de markt die verschillende soorten producten leveren en het eenvoudig maken om informatie uit open bronnen te verzamelen en te verwerken. Hierbij kan gedacht worden aan pakketten zoals 'SpiderFoot', 'Recon-ng', 'Maltego' of 'Spyse'.[14] Het zijn dit soort tools die het onderwerp kunnen zijn van dit rapport.

Sommige tools bevatten modules of plug-ins voor verschillende OSINT toepassingen. Dit kunnen gratis of betaalde modules of plug-ins zijn. Met behulp van een plug-in of module kan een gebruiker met een aantal muisklikken een bron, zoals Facebook of LinkedIn, geautomatiseerd bevragen. Deze plug-ins of modules kunnen ook bestaan uit samengestelde datasets. Het verdienmodel van deze bedrijven ligt in het aanbieden van deze betaalde modules of plug-ins.

---

13 Zie ook toezichtsrapport nr. 39 (2014) over het gebruik van gegevens van sociale media en internetforums door de AIVD.

14 Zie www.tools.kali.org/information-gathering/recon-ng; www.maltego.com; en www.spyse.com. SpiderFoot wordt bijvoorbeeld geschreven als: *"'a reconnaissance tool that automatically queries over 100 public data sources (OSINT) to gather intelligence on IP addresses, domain names, e-mail addresses, names and more"* (http://spiderfoot.net/documentation/).

Commerciële partijen bieden ook gespecialiseerde datasets aan, die door henzelf zijn geaggregeerd. Deze datasets bevatten soms gegevens die zijn 'gescrapet' van het internet. Dat wil zeggen dat de gegevens automatisch op basis van vooraf ingestelde parameters van publiek toegankelijke bronnen worden verzameld.[15] De aanbieders van deze datasets kunnen terughoudend zijn ten aanzien van het verstrekken van informatie over de herkomst van deze datasets en over de wijze waarop deze datasets zijn opgebouwd. Gegevens die door de aanbieders van apps of websites over gebruikers worden gegenereerd (bijvoorbeeld via cookies en advertenties) worden vaak aan andere partijen doorverkocht of met andere partijen uitgewisseld. Vervolgens kunnen deze gegevens in een commerciële dataset terechtkomen die via een tool voor automated OSINT kunnen worden geraadpleegd.

De datasets die worden aangeboden door dit soort partijen kunnen onder meer bestaan uit:
- Gescrapete (historische) data: het gaat hierbij om data van meerdere sociale media-bronnen, maar veel commerciële partijen scrapen ook data van internetfora of marktplaatsen op het dark web;
- Cryptovaluta: informatie over crypto-valutatransacties (tokens, adressen en gebruikers);
- Gelekte datasets: sets bestaande uit data die bijvoorbeeld via een hack zijn verkregen. Gelekte datasets kunnen via open bronnen beschikbaar zijn gesteld of alleen via een commerciële partij;
- Advertentiedata: datasets met bijvoorbeeld locatiegegevens die verzameld worden door het aankopen van een advertentieplaats in een app of op een website.[16]

Aanbieders van tools voor automated OSINT verzamelen deze gegevens, verwerken deze verder en bieden ze aan als 'databron' aan klanten, zoals inlichtingen- en veiligheidsdiensten. Gegevens uit verschillende datasets met persoonsgegevens kunnen door de aanbieder zijn bewerkt en samengevoegd tot één dataset. Eén samengestelde dataset kan miljarden gegevens bevatten.

Tot de commercieel aangeboden datasets waartoe via de gespecialiseerde tools toegang kan worden verkregen, behoort 'advertisement-based intelligence' (ADINT). Dit betreffen gegevens van mobiele apparaten, zoals locatiegegevens en gegevens over het mobiele apparaat. Deze gegevens worden gegenereerd door advertenties in apps, waarna deze gegevens op een (data)markt worden verhandeld. De aanbieders van deze gegevens worden ook wel datahandelaren ('data brokers') genoemd.

Voor zover deze commercieel beschikbare gegevens niet als een 'voor een ieder toegankelijke informatiebron' kunnen worden gezien, zijn de diensten op basis van artikel 25 lid 1 onder b Wiv 2017 bevoegd om commercieel beschikbaar gestelde gegevens te verwerken in het kader van hun taakuitoefening.[17] De CTIVD merkt op dat de reikwijdte van deze bevoegdheid niet duidelijk uit het wetsartikel is af te leiden, omdat daarin wordt gesproken over 'informatiebronnen waarvoor aan de dienst een recht op kennisneming van de aldaar berustende gegevens is verleend'. Een 'recht op kennisname' blijkt doorgaans uit een grondslag in andere wetgeving, zoals in de Wet politiegegevens, op basis waarvan de AIVD en de MIVD de aldaar berustende gegevens kunnen raadplegen. In de memorie van toelichting bij de Wiv 2017 wordt één keer opgemerkt dat de diensten op grond het wetsartikel ook 'commercieel beschikbaar gestelde gegevens' kunnen verzamelen, waarbij alleen gegevens van de Kamer van Koophandel als voorbeeld worden genoemd.[18] Meer duidelijkheid over de reikwijdte van deze wettelijke grondslag voor de verwerking van commercieel beschikbaar gestelde gegevens en passende wettelijke waarborgen zijn daarom gewenst.

15 Zie o.a., H. Gibson, 'Acquisition and Preparation of Data for OSINT Investigations', in: B. Akhgar, S. Bayerl & F. Sampson, *Open Source Intelligence Investigation*, Springer: 2016.
16 P. Vines, F. Roesner en T. Kohno, 'Exploring ADINT: Using Ad Targeting for Surveillance on a Budget – or – How Alice Can Buy Ads to Track Bob', *The 16th ACM Workshop on Privacy in the Electronic Society (WPES 2017)*. Zie tevens H. Gibson, 'Acquisition and Preparation of Data for OSINT Investigations', in: B. Akhgar, S. Bayerl & F. Sampson, *Open Source Intelligence Investigation*, Springer: 2016.
17 Artikel 25 lid 1 sub b Wiv 2017. Zie ook *Kamerstukken II* 2016/17, 34588, nr. 3, p. 38. Zie ook paragraaf 1.2 van het toetsingskader (Bijlage I).
18 *Kamerstukken II* 2016/17, 34588, nr. 3, p. 38.

2.4 Selectie van tools door de diensten

Wanneer een organisatie besluit om automated OSINT tools in te zetten, kan zij ervoor kiezen deze tools zelf te (laten) ontwikkelen. Dit heeft als voordeel dat een 'tailor-made' tool beschikbaar komt waarvan alle functionaliteiten en achterliggende bronnen bekend zijn. Echter, daar staat de noodzaak van het in huis hebben van geavanceerde kennis, ontwikkeltijd en kosten tegenover. Een marktproduct dat al is ontwikkeld heeft deze beperkingen niet, maar kent andere nadelen. Deze nadelen kunnen eruit bestaan dat er geen inzicht is in de exacte werking van de tool en dat er slechts beperkt invloed kan worden uitgeoefend op functionaliteiten (zoals zoekmogelijkheden en logging). In voorkomende gevallen kunnen datasets niet los van de tool worden aangeschaft; dit is onderdeel van het verdienmodel.

Beslissingen over de aanschaf van de tools voor automated OSINT vragen om een zorgvuldig wegingsproces. Als de AIVD of de MIVD geïnteresseerd is in een bepaald product op het gebied van automated OSINT, dan wordt deze niet eerst beoordeeld op basis van vooraf binnen de dienst vastgelegde criteria.

Uit het onderzoek blijkt dat door de diensten veel aandacht is besteed aan de mogelijke meerwaarde van de tools ten opzichte van andere mogelijkheden van openbronnenonderzoek. Daarbij is goed nagegaan wat het doel is van het middel en welke gegevens daarbij worden verzameld. Er is met name aandacht voor de operationele meerwaarde van het specifieke product en de operationele veiligheid (ook van medewerkers) (zie paragraaf 3.5), en minder voor de inbreuken die de inzet van de tool met zich mee zou kunnen brengen op de fundamentele rechten van betrokkenen.

In het kader van de zorgplicht voor een zorgvuldige gegevensverwerking (artikel 24 Wiv 2017) dient er ook aandacht te worden besteed aan compliance-aspecten zoals 'dashboarding' en logging. Ook de zorgvuldigheid van de gegevensverwerking (zie paragraaf 3.2) dient in een beoordeling te worden meegenomen. Het verkrijgen van zicht op deze aspecten draagt bij aan een gedegen kennisniveau van de werking van de tools en de aard van de achterliggende datasets beschikken. Deze kennis is noodzakelijk bij het afwegen van de proportionaliteit van de gegevensverwerkingen die met het gebruik van de tools plaatsvinden. Daarnaast is deze kennis nodig om te bepalen welke maatregelen genomen moeten worden in het kader van de zorgplicht voor de gegevensverwerking en het realiseren van interne controle met effectief toezicht.

2.5 Gebruik van automated OSINT-tools bij de AIVD

De AIVD heeft in de onderzoeksperiode van 1 juli 2020 tot en met 31 maart 2021 zeer beperkt gebruik gemaakt van tools voor automated OSINT. Het gebruik van deze tools is voorbehouden aan een aantal aangewezen functionarissen.

Tijdens de onderzoeksperiode heeft één AIVD-team, dat zich richt op het onderkennen van nieuwe targets die de nationale veiligheid bedreigen, enige ervaring opgedaan met het gebruik van een – extern aangeschafte – tool voor automated OSINT. Het doel was na te gaan of de tool een meerwaarde heeft voor de operationele praktijk. Uit een interne evaluatie van de AIVD blijkt dat de automated OSINT-tool inderdaad meerwaarde heeft, omdat het efficiënter onderzoek mogelijk maakt door automatisch vele bronnen tegelijk te bevragen. In korte tijd kunnen medewerkers meer gegevens over een persoon verzamelen. Deze tool bevond zich in de onderzoeksperiode (en tot aan het vaststellen van dit rapport) in een testfase. Wel is de tool tijdens de onderzoeksperiode twee keer in het operationele proces ingezet. Daarbij is één keer de bevoegdheid op grond van artikel 38 Wiv 2017 voor het stelselmatig verzamelen van persoonsgegevens uit voor een ieder toegankelijke informatiebronnen ingezet.

Daarnaast hebben data-analisten van de dienst gebruik gemaakt van een tweede – extern aangeschafte – tool voor automated OSINT om gegevens over targets te verwerken. Het is één van de tools die data-analisten voor hun werkzaamheden ter beschikking hebben. Tijdens de onderzoeksperiode is meerdere keren van de tool gebruik gemaakt op basis van de algemene bevoegdheid in artikel 25 Wiv 2017.

De AIVD heeft ook een afdeling met gespecialiseerde medewerkers die in opdracht van een team diepgaander openbronnenonderzoek uitvoeren. Het gaat daarbij vaak om 'targetgericht' onderzoek, waarbij gegevens worden verzameld over een persoon of organisatie die in de aandacht van de dienst staat. Dit team heeft ten tijde van het onderzoek geen gebruik gemaakt van tools voor automated OSINT.

Ten slotte voeren medewerkers met bepaalde functies bij (bijna) alle teams van de AIVD tot een bepaalde diepgang openbronnenonderzoek uit, zonder gebruik van tools voor automated OSINT.

De beperkte inzet van tools voor automated OSINT laat zich verklaren doordat de AIVD tijdens de onderzoeksperiode met name heeft getest of tools voor automated OSINT meerwaarde hebben voor de organisatie. Daarmee zijn de tools dus (nog) geen onderdeel van een vast proces bij het verzamelen van gegevens via openbronnenonderzoek door medewerkers van teams of door de gespecialiseerde medewerkers van de afdeling OSINT.

2.6 Gebruik van automated OSINT-tools bij de MIVD

De MIVD heeft in de onderzoeksperiode van 1 juli 2020 tot en met 31 maart 2021 veelvuldig gebruik gemaakt van tools voor automated OSINT.

De tools voor automated OSINT worden ingezet door een gespecialiseerd bureau bij de MIVD en het gebruik ervan is een vast onderdeel van het inlichtingenproces van de medewerkers die gespecialiseerd zijn in OSINT. Dit bureau met gespecialiseerde medewerkers voert in opdracht van teams openbronnenonderzoek uit. De diepgang van het onderzoek (ook met automated OSINT tools) is afhankelijk van de vraag die het team stelt of van de inlichtingenbehoefte.

Het gespecialiseerde bureau van de MIVD maakte tijdens de onderzoeksperiode gebruik van meerdere – extern aangeschafte - tools voor automated OSINT. Deze zijn ongeveer twee tot drie jaar geleden aangeschaft. Het onderzoek met gebruik van tools voor automated OSINT vindt vaak plaats aan de hand van een eenvoudige opdracht, zoals de vraag of aan een target een profiel op een sociale mediadienst is te koppelen. Het kan echter ook gaan om een uitgebreid onderzoek, waarbij op voorhand voorzienbaar is dat een 'min of meer volledig beeld van bepaalde aspecten van het privéleven van een persoon' wordt verkregen. In dat geval moet de bevoegdheid tot het stelselmatig verzamelen van persoonsgegevens uit voor een ieder toegankelijke informatiebronnen worden ingezet (artikel 38 Wiv 2017).

Ten slotte hebben bijna alle teams van de MIVD medewerkers aangewezen die tot een bepaalde diepgang openbronnenonderzoek uitvoeren, maar zij maken daarbij geen gebruik van tools voor automated OSINT.

2.7 Verschillen automated OSINT AIVD en MIVD

De algemene observatie van de CTIVD is dat de OSINT-afdeling bij de MIVD verder is gevorderd in automated OSINT dan de AIVD. Ter illustratie: bij de MIVD is 73 keer en bij de AIVD is één keer de

bevoegdheid van artikel 38 Wiv 2017 ingezet voor het stelselmatig verzamelen van gegevens omtrent een persoon uit voor ieder toegankelijke informatiebronnen, met behulp van een automated OSINT tool. Eén enkele inzet van de bevoegdheid ex artikel 38 Wiv 2017 kan zich ook richten op een (beperkt en specifiek aangegeven) aantal personen.

Het grote verschil in het aantal aanvragen voor stelselmatig openbronnenonderzoek met behulp van tools voor automated OSINT (73 bij de MIVD ten opzichte van één keer bij de AIVD) is verklaarbaar, omdat het gebruik van tools voor automated OSINT bij de MIVD deel uitmaakt van het vaste inlichtingenproces van het OSINT-bureau en daarmee meer ervaring is opgedaan met het gebruik ervan. De tools zitten bij de AIVD al langere tijd in een 'testfase', waarbij slechts een zeer beperkt aantal medewerkers toegang hebben tot de automated OSINT-tools.

3. Automated OSINT: Toetsing wettelijk kader

In dit hoofdstuk toetst de CTIVD in hoeverre de AIVD en de MIVD de werking van de tools voor automated OSINT en de herkomst en de aard van de achterliggende bronnen in voldoende mate hebben doorgrond met het oog op de naleving van de bepalingen omtrent gegevensverwerking.

De CTIVD toetst daarbij specifiek aan de volgende wettelijke bepalingen:

- De bepalingen omtrent gegevensverwerking in de Wiv 2017 (artikel 18 Wiv 2017 e.v.);
- De hoofden van de dienst 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 zijn met de wet (artikel 24 Wiv 2017).

Voorafgaand aan de ontwikkeling of de inzet van een tool voor automated OSINT moeten de diensten zich afvragen hoe de toekomstige gegevensverwerking zich verhoudt tot de Wiv 2017. De werking van een tool en de herkomst en de aard van de bronnen die daarbij worden geraadpleegd, hebben namelijk invloed op de ernst van de inbreuk op de fundamentele rechten van de betrokkenen en daarmee op de uit te voeren proportionaliteitstoets. Ook is deze informatie belangrijk om vooraf in te schatten of het onderzoek mogelijk stelselmatig is. Bovendien kan op basis van deze informatie het hoofd van de dienst zorg dragen voor een zorgvuldige gegevensverwerking en indien nodig maatregelen treffen (artikel 24 Wiv 2017).

3.1 Algemene bepalingen omtrent gegevensverwerking

De diensten moeten bij de verwerking van gegevens met tools voor automated OSINT voldoen aan de algemene bepalingen omtrent gegevensverwerking. De verplichtingen in artikel 18 Wiv 2017 staan daarbij centraal. In artikel 18 Wiv 2017 zijn algemene principes omtrent gegevensverwerking neergelegd. Artikel 18 lid 1 Wiv 2017 schrijft voor dat gegevens slechts voor een bepaald doel en slechts voor zover noodzakelijk voor de goede taakuitvoering van de Wiv 2017 (of de Wet veiligheidsonderzoeken) mogen worden verwerkt. Artikel 18 lid 2 Wiv 2017 schrijft voor de verwerking van gegevens geschied in overeenstemming met de wet en op 'behoorlijke en zorgvuldige wijze' plaatsvindt. Dit laatste houdt ook in dat toetsing op noodzaak en proportionaliteit moet plaatsvinden. Artikel 18 lid 3 Wiv 2017 schrijft voor dat gegevens die in het kader van taakuitvoering van de diensten worden verwerkt, 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.

Voor de toetsing op noodzaak, proportionaliteit en betrouwbaarheid en juistheid van de gegevens is het noodzakelijk dat - voordat een tool voor automated OSINT in gebruik wordt genomen - de werking van de tool duidelijk is en de achterliggende databronnen zo goed mogelijk worden doorgrond.

3.2 Behoorlijke en zorgvuldige gegevensverwerking

Een behoorlijke en zorgvuldige gegevensverwerking brengt ook met zich mee dat wordt nagegaan wat het doel is van de verwerking, of de gegevensverwerking noodzakelijk is om dat doel te bereiken en of de gegevensverwerking proportioneel is, gelet op de inbreuk die wordt gemaakt op de fundamentele rechten van de betrokkene(n). Voorafgaand aan de ingebruikname van de tools voor automated OSINT zijn er geen afwegingen gemaakt van de proportionaliteit. De diensten zijn nagegaan welke

operationele waarde de tools met achterliggende bronnen voor hen hebben en hebben daarmee aan het doel- en noodzakelijkheidsvereiste getoetst, maar hebben onvoldoende aandacht besteed aan de impact op de fundamentele rechten van betrokkenen.

Kennis vooraf over de werking (de functionaliteiten) en achterliggende bronnen van de tools is noodzakelijk om de proportionaliteitstoets uit te kunnen voeren. Natuurlijk kunnen medewerkers ook bij het overnemen van gegevens een afweging maken tussen het belang de gegevens te verwerken voor het betreffende inlichtingenonderzoek en de ernst van de inbreuk op de fundamentele rechten van de betrokkene, maar dat is niet voldoende. Op basis van een voorafgaande toets en later op basis van de ervaringsleer kan bijvoorbeeld een inschatting worden gemaakt of gevoelige gegevens worden verwerkt door het gebruik van (bepaalde bronnen in) tools voor automated OSINT. Gevoelige gegevens mogen slechts worden overgenomen als dat in aanvulling is op de verwerking van andere gegevens en slechts voor zover dat voor het doel van de gegevensverwerking onvermijdelijk is (artikel 19 Wiv 2017). Ook kan worden besloten in voorkomende gevallen bepaalde functionaliteiten van het tool niet te gebruiken of bepaalde resultaten niet over te nemen, bijvoorbeeld wanneer het kan leiden tot een stelselmatige inzet als gevolg van het verwerken van grote hoeveelheden locatiegegevens.

De reden dat een aparte toets – voorafgaand aan de ingebruikname van de tool – noodzakelijk is, is dat de functionaliteiten van een tool en de aard van bronnen een verschillende impact op de fundamentele rechten (met name het recht op privacy) met zich kunnen meebrengen. De inbreuk op de fundamentele rechten van betrokken personen is bijvoorbeeld gering voor wat betreft het overnemen van gegevens uit nieuwsberichten en gegevens op publiek toegankelijke delen van sociale mediadiensten.[19] Dit zijn de bronnen die in de memorie van toelichting uit de Wiv 2017 worden genoemd. De tools voor automated OSINT waar de AIVD en de MIVD gebruik van maken, kunnen (zoals eerder aangegeven) echter ook locatiegegevens en gelekte datasets bevatten. 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.[23]

Met een systematische aanpak *vooraf*, kan een afweging worden gemaakt van de inbreuk op de fundamentele rechten die kan plaatsvinden bij de verwerking van gegevens met de tool en kan - in het kader van de zorgplicht in artikel 24 Wiv 2017 – worden beslist welke technische, personele of organisatorische maatregelen moeten worden genomen om een zorgvuldige gegevensverwerking te bewerkstelligen. Het is bijvoorbeeld denkbaar dat als organisatorische maatregel slechts medewerkers van een bepaalde afdeling of bepaalde functie gebruik mogen maken van de tools voor automated

19 *Kamerstukken II* 2016/17, 34588, nr. 3, p. 39 en 55-56.
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 Zie ook het rapport nr. 55 (2018) en het Toetsingskader over door derden op internet aangeboden bulkdatasets.
22 Per 1 maart 2019 is de Wet computercriminaliteit III in werking getreden (*Stb*. 2019, 67). Artikel 138c Sr stelt het overnemen of doorgeven van gegevens uit een niet-openbare bron strafbaar en artikel 139g Sr stelt heling van gegevens strafbaar.
23 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 openbaarheid is gekomen.

OSINT. Uit paragrafen 2.5 en 2.6 blijk overigens dat deze laatst genoemde organisatorische maatregel reeds door de beide diensten wordt toegepast.

3.3 Betrouwbaarheid en juistheid van gegevens

De gegevens die in het kader van de uitvoering met tools voor automated OSINT worden verwerkt, dienen te zijn voorzien van een aanduiding omtrent de mate van betrouwbaarheid of een verwijzing naar het document of de bron waaraan de gegevens zijn ontleend (artikel 18 lid 3 Wiv 2017). Bovendien draagt het hoofd van de dienst er zorg voor voorzieningen te treffen ter bevordering van de juistheid en volledigheid van de gegevens, alsmede kwaliteit van de gegevensverwerking (artikel 24 lid 2 onderdeel a Wiv 2017).

De herkomst en juistheid van de gegevens in achterliggende databronnen die met de tools kunnen worden geraadpleegd, zijn niet altijd duidelijk. De herkomst van gegevens is bijvoorbeeld lastiger te verifiëren als deze bestaan uit door de aanbieder samengestelde datasets of commercieel aangeboden locatiegegevens. Tegelijkertijd kunnen de tools voor automated OSINT ook bijdragen aan het bevorderen van de juistheid en volledigheid van de gegevens, omdat daarmee meerdere gegevensbronnen kunnen worden geraadpleegd. Hierdoor kan een resultaat uit één bron worden geverifieerd met een resultaat uit een andere bron, voordat gegevens eventueel worden overgenomen in een rapport.

Uit het onderzoek van de CTIVD is gebleken dat een voorafgaande toets op de betrouwbaarheid en juistheid van gegevens, voorafgaand aan de ingebruikname van de automated OSINT-tools, niet in voldoende mate heeft plaatsgevonden. Wel worden door medewerkers van de AIVD en de MIVD de resultaten uit een zoekslag met een tool voor automated OSINT zo nodig gevalideerd met de resultaten uit een andere tool of databron, als wordt getwijfeld aan de juistheid van de gegevens. Ook vermelden medewerkers in een rapportage na gebruik van de tool de achterliggende bronnen waarop een overgenomen resultaat is gebaseerd. Dat is positief, maar niet voldoende voor een goede naleving van de algemene bepalingen omtrent gegevensverwerking.

De diensten dienen *voorafgaand* aan de ingebruikname van een tool de werking (de functionaliteiten) van de tool en achterliggende bronnen te doorgronden. Met een systematische aanpak vooraf is het mogelijk vooraf de betrouwbaarheid van bepaalde bronnen te beoordelen en – in het kader van de zorgplicht in artikel 24 Wiv 2017 – te beslissen welke personele, organisatorische of technische maatregelen genomen moeten worden om de gegevensverwerking in overeenstemming met de wet te brengen. Het is bijvoorbeeld denkbaar als personele maatregel geautoriseerde medewerkers in een instructie kennis mee te geven over hoe moet worden omgegaan met bepaalde achterliggende bronnen bij een tool voor automated OSINT.

3.4 Geautomatiseerde data-analyse

Op de gegevensverwerking via tools voor automated OSINT is artikel 60 Wiv 2017 onverkort van toepassing. Dit betekent, eenvoudig gesteld, dat als er sprake is van geautomatiseerde data-analyse er geen geautomatiseerde besluitvorming mag plaatsvinden.[24] Tijdens de verwerking van gegevens met tools voor automated OSINT vindt geautomatiseerde data-analyse plaats, omdat er onder meer sprake is van bestandsvergelijking op basis van een zoekvraag met gegevens op de achterliggende bronnen.

24 Artikel 60 lid 3 Wiv 2017.

Het beleid en werkwijze van de diensten brengt met zich mee dat géén maatregelen jegens een persoon worden genomen uitsluitend op basis van een zoekslag in de tool. De resultaten van een zoekslag in de tool(s) voor automated OSINT worden verwerkt in een rapportage die door een medewerker wordt opgesteld. Pas op basis van deze rapportage kunnen, veelal in combinatie met andere gegevens, eventueel maatregelen jegens een persoon worden genomen. Met deze werkwijze wordt op een rechtmatige wijze invulling gegeven aan het verbod op geautomatiseerde besluitvorming in artikel 60 Wiv 2017.

3.5 Naleving zorgplicht bron en identiteit medewerkers

Voordat een automated OSINT tool in gebruik werd genomen, besteedden de AIVD en de MIVD nadrukkelijk aandacht aan operationele risico's (zoals het door ongeautoriseerde personen op de hoogte raken van operaties) en de veiligheid van de medewerkers van de diensten. Ook het risico dat de identiteit bekend wordt van personen of organisaties waar onderzoek die onderwerp van onderzoek zijn, is geadresseerd en werd van een risico-inschatting voorzien.

Binnen het onderzoek is vastgesteld dat de AIVD en de MIVD voldoende aandacht hebben gehad voor de bescherming van de identiteit van de personen of organisaties die in onderzoek zijn bij de diensten, de identiteit van medewerkers die de zoekvragen uitvoeren en de gebruikte databronnen bij automated OSINT.

Het hoofd van de dienst draagt zorg voor de geheimhouding van de daarvoor in aanmerking komende gegevens en de veiligheid van de personen met wier medewerking gegevens worden verzameld (artikel 23 Wiv 2017). De CTIVD stelt vast dat de hoofden van de diensten de zorgplicht op geheimhouding en de veiligheid van personen bij automated OSINT goed zijn nagekomen.

3.6 Naleving zorgplicht omtrent gegevensverwerking

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 zijn met de wet (artikel 24 Wiv 2017). Tijdens de onderzoeksperiode heeft geen voorafgaande afweging en beoordeling met betrekking tot de privacyrisico's bij automated OSINT plaatsgevonden.

Uit de bevindingen in hoofdstuk 2 over de inrichting van het proces van automated OSINT en de bevindingen in dit hoofdstuk over de voorafgaande toets op de naleving van de algemene bepalingen omtrent gegevensverwerking blijkt dat de beide diensten tot op zekere hoogte (meer algemene) personele, technische en organisatorische maatregelen hebben getroffen om een zorgvuldige gegevensverwerking te waarborgen. Daarbij wijst de CTIVD op de personele en organisatorische maatregelen zoals de specifiek aangewezen medewerkers die meer diepgaand OSINT-onderzoek uitvoeren, eventueel met gebruik van de tools voor automated OSINT. Ook worden de bevindingen uit OSINT gedocumenteerd en wordt tot op zekere hoogte tijdens het onderzoek een toets op de betrouwbaarheid en juistheid van de gegevens uitgevoerd.

Desondanks stelt de CTIVD ook tekortkomingen vast in het beleid, procedures en werkinstructies van de diensten (waarbij het gaat om de genomen organisatorische maatregelen). Dit is *onzorgvuldig*. Bij de AIVD is een belangrijke tekortkoming gelegen in de gebrekkige uitwerking van het criterium van stelselmatigheid in de context van automated OSINT. Dit criterium is belangrijk, omdat de bevoegdheid in artikel 38 Wiv 2017 schriftelijk en gemotiveerd moet worden aangevraagd, met andere woorden: er moet toestemming worden gevraagd voor de inzet, wanneer op voorhand redelijk voorzienbaar is dat met het overnemen van de persoonsgegevens uit voor een ieder toegankelijke informatiebronnen

een 'min of meer volledig beeld van bepaalde aspecten van het privéleven van de betrokkene wordt verkregen'.[25]

De AIVD stelt in haar beleid dat één zoekslag in het systeem op een naam van een target met een tool voor automated OSINT nooit stelselmatig is. Het is echter denkbaar dat een 'eenvoudige naslag' met behulp van de onderzochte tools een grote hoeveelheid en diversiteit aan gegevens over een persoon oplevert, met als gevolg een min of meer volledig beeld van bepaalde aspecten van het privéleven. Door vervolgens gegevens over het target over te nemen, bijvoorbeeld van verschillende sociale mediadiensten en gegevens uit verschillende datasets, kan het onderzoek wel degelijk stelselmatig van aard zijn. Van tevoren moet op basis van het doel van het onderzoek, de kennis over de tools en achterliggende bronnen en de ervaringsleer een inschatting worden gemaakt of de raadpleging en daaropvolgende overname van de gegevens stelselmatig zal zijn.

De MIVD heeft ruim aandacht besteed aan het criterium van stelselmatigheid in haar beleid en werkinstructies voor OSINT (meer uitgebreid dan de AIVD). Toch constateert de CTIVD in het beleid en werkinstructie een belangrijke tekortkoming. Het beleid van de MIVD bevat namelijk een uitzondering op het criterium van stelselmatigheid door te stellen dat het overnemen van "zakelijke informatie" over 'strijders' nooit stelselmatig zal zijn. Het zou om zakelijke informatie gaan wanneer het doel van de naslag is om inzicht te verkrijgen in de modus operandi, werkzaamheden en het zakelijk netwerk van de strijder. Het op deze wijze inperken van de reikwijdte van het begrip stelselmatigheid heeft geen wettelijke grondslag. Zo neemt de kans op onrechtmatigheden in de praktijk toe, omdat bijvoorbeeld ten onrechte het toestemmingsvereiste voor het stelselmatig verzamelen van persoonsgegevens uit voor een ieder toegankelijke informatiebronnen niet wordt toegepast. Tijdens het onderzoek van de CTIVD is deze uitzondering door de MIVD in het beleid en de werkinstructies verwijderd.

25 Zie ook het Toetsingskader (Bijlage I).

4. Conclusie en aanbevelingen

De Wet op de inlichtingen- en veiligheidsdiensten (Wiv 2017) biedt de AIVD en de MIVD de mogelijkheid om publiek toegankelijke (persoons)gegevens te verzamelen en te verwerken. Dit wordt ook wel openbronnenonderzoek genoemd of aangeduid met de term OSINT ('open source intelligence'). OSINT wordt door de wetgever niet als een indringend inlichtingenmiddel gezien. Het betreft een algemene bevoegdheid van de diensten, waarbij er een onderscheid is tussen een niet-stelselmatige en stelselmatige inzet. Voor het stelselmatig verzamelen van persoonsgegevens uit voor een ieder toegankelijke informatiebronnen is toestemming vereist.

Wanneer openbronnenonderzoek geautomatiseerd plaatsvindt met behulp van specialistische software of webapplicaties, is er sprake van 'automated OSINT'. In dit onderzoek worden daarbij twee elementen onderscheiden: de *tools* die worden gebruikt en de *bronnen* (datasets) die via deze tools geraadpleegd kunnen worden. Bij de 'tools' gaat het om software met zoekfuncties en netwerkanalysefuncties, waarbij een grote diversiteit aan bronnen kan worden bevraagd. Deze tools kunnen afkomstig zijn van commerciële aanbieders of door de diensten zelf zijn ontwikkeld.

De CTIVD beoogt met dit onderzoek de volgende onderzoeksvraag te beantwoorden:
Hebben de AIVD en de MIVD de werking van de tools voor automated OSINT en de herkomst en de aard van de achterliggende bronnen in voldoende mate doorgrond met het oog op de naleving van de bepalingen omtrent gegevensverwerking?

De rechtmatigheidstoets van de CTIVD richt zich in dit onderzoek primair op OSINT-tools en de via deze tools te raadplegen datasets (de bronnen). Hoe deze tools en bronnen in concrete gevallen worden ingezet is geen onderdeel van het onderzoek. De CTIVD acht het essentieel dat de diensten het proces van automated OSINT inrichten zodat deze in overeenstemming is met de Wiv 2017. Hiervoor is het nodig dat de diensten voldoende zicht krijgen op de werking van de tools, zoals de functionaliteiten die de tools bieden en de achterliggende bronnen. Met deze kennis kunnen zij bezien hoe de tools en bronnen zich verhouden tot de wettelijke vereisten voor gegevensverwerking en de wettelijke bevoegdheid openbronnenonderzoek uit te voeren (al dan niet stelselmatig).

Hoofdstuk 2 schetst op hoofdlijnen de verschillende manieren waarop (automated) OSINT in het algemeen en meer specifiek binnen de AIVD en de MIVD plaatsvindt. Hoofdstuk 3 geeft de bevindingen weer over de naleving van wettelijke vereisten omtrent gegevensverwerking in de praktijk van automated OSINT bij de AIVD en de MIVD.

Conclusies hoofdstuk 2

Uit hoofdstuk 2 blijkt dat zowel de AIVD als de MIVD tijdens de onderzoeksperiode gebruik hebben gemaakt van meerdere commerciële tools voor de uitvoering van automated OSINT. De MIVD maakt op veel grotere schaal gebruik van deze tools dan de AIVD. Ter illustratie: de MIVD heeft tijdens de onderzoeksperiode van 1 juli 2020 tot en met 31 maart 2021 in totaal 73 keer de bevoegdheid tot het stelselmatig verzamelen van persoonsgegevens met een tool voor automated OSINT ingezet en de AIVD slechts één keer.

Tools voor automated OSINT bieden twee grote voordelen ten opzichte van regulier openbronnenonderzoek via een webbrowser. Het eerste grote voordeel is het gebruiksgemak; in één zoekslag met een tool voor automated OSINT kunnen tot wel honderden bronnen tegelijkertijd worden bevraagd. De resultaten kunnen vervolgens door de tools worden gevisualiseerd. Het tweede grote voordeel voor het gebruik van de tools voor de diensten is gelegen in het feit dat gegevens kunnen worden geraadpleegd die op commerciële basis op een gebruikersvriendelijke manier door de leverancier worden aangeboden. Een voorbeeld daarvan betreffen gelekte gegevens van gebruikers van sociale

mediadiensten. Leveranciers kunnen deze datasets samenvoegen als één raadpleegbare bron (een 'samengestelde dataset') met soms wel miljarden gegevens.

Een voorbeeld van commerciële gegevens die via deze tools kunnen worden geraadpleegd, betreffen locatiegegevens die worden gegenereerd door advertenties die worden getoond aan gebruikers van applicaties. De aanbieders van commerciële tools voor OSINT kunnen advertentiegegevens afnemen bij datahandelaren ('data brokers') en deze via hun tool beschikbaar stellen aan klanten, waaronder inlichtingen- en veiligheidsdiensten.

Het nadeel van een marktproduct is dat niet altijd inzicht is in de exacte werking van de tool en dat er slechts beperkt invloed kan worden uitgeoefend op functionaliteiten (zoals zoekmogelijkheden en logging). In voorkomende gevallen kunnen datasets niet los van de tool worden aangeschaft; dit is onderdeel van het verdienmodel.

De omvang, aard en diversiteit aan persoonsgegevens in deze automated OSINT tools kan een ernstiger inbreuk op fundamentele rechten met zich meebrengen, in het bijzonder op het recht op privacy, dan het raadplegen van gegevens in voor een ieder toegankelijke informatiebronnen op internet, zoals gegevens via een zoekmachine of publiek toegankelijke gegevens op sociale media.

Uit de memorie van toelichting van de Wiv 2017 kan worden opgemaakt dat destijds geen rekening is gehouden met deze automated OSINT-praktijk, die zich in de nabije toekomst verder zal blijven ontwikkelen. OSINT is nadrukkelijk niet meer alleen het 'naslaan' van telefoonboeken of zoeken van gegevens op internet met een zoekmachine. Het onderhavige onderzoek weerspiegelt het volgende: met automated OSINT kunnen honderden bronnen van diverse herkomst tegelijkertijd worden geraadpleegd, waaronder locatiegegevens of gegevens uit gelekte datasets. De huidige praktijk van automated OSINT brengt een ernstiger privacy-inbreuk met zich mee dan tijdens de totstandkoming van de wet is voorzien.

Deze bevindingen leiden tot **aanbeveling 1:**
Gezien de aard, diversiteit en hoeveelheid van de in het geding zijnde gegevens beveelt de CTIVD de wetgever aan een meer voorzienbare wettelijke grondslag met voldoende waarborgen te creëren ten aanzien van automated OSINT, zowel voor wat betreft de tools als de via deze tools te raadplegen bronnen.

Conclusies hoofdstuk 3

In hoofdstuk 3 is nagegaan in hoeverre de diensten bij de verwerking van gegevens met tools voor automated OSINT voldoen aan de algemene bepalingen omtrent gegevensverwerking. De plicht tot een behoorlijke en zorgvuldige gegevensverwerking in artikel 18 Wiv 2017 staat daarin centraal. Voordat een tool voor automated OSINT in gebruik wordt genomen, is het van belang dat de werking (de functionaliteiten) van de tool duidelijk is en dat de achterliggende databronnen zo goed mogelijk worden doorgrond. Met deze kennis kan worden nagegaan welke gegevens op welke manier worden verwerkt. Deze informatie is noodzakelijk voor de uitvoering van de noodzakelijkheids- en proportionaliteitstoets en om na te gaan wat de betrouwbaarheid en juistheid van de gegevens zijn die worden verwerkt door de tools. Gevoelige gegevens mogen slechts worden verwerkt in aanvulling op de verwerking van andere gegevens en slechts voor zover dat onvermijdelijk is (artikel 19 Wiv 2017) (zie paragraaf 3.1-3.3).

Het antwoord op de onderzoeksvraag is dat de AIVD en MIVD de werking van de tools voor automated OSINT en de herkomst en de aard van de via deze tools te raadplegen bronnen in onvoldoende mate hebben doorgrond om zodoende aan de bepalingen in de Wiv 2017 met betrekking tot gegevensverwerking te kunnen voldoen. In de praktijk houden de diensten al wel voldoende rekening met operationele - en beveiligingsaspecten bij de inzet van tools voor automated OSINT (zie paragraaf 3.5). In het kader van de zorgplicht voor een zorgvuldige gegevensverwerking moeten de

diensten (alsnog) de werkwijzen en achterliggende bronnen van de tools in kaart brengen en daarop mitigerende maatregelen nemen om onrechtmatigheden in de toekomst te voorkomen (zie paragraaf 3.6). De CTIVD stelt vast dat meerdere verbeteringen noodzakelijk zijn om automated OSINT in overeenstemming met de wet te brengen.

Deze bevinding leiden tot **aanbeveling 2:**
De AIVD en de MIVD dienen zich bij de selectie en verwerving van tools voor automated OSINT (en daarmee ook de achterliggende bronnen) ook te richten op het waarborgen van een zorgvuldige gegevensverwerking. Het verdient de voorkeur dat de diensten in gezamenlijkheid een beleidskader ontwikkelen met bijbehorende werkinstructies.

In het belang van rechtszekerheid, de rechtmatigheid en de slagkracht van de diensten (vanwege de continuïteit van de rechtmatige gegevensverwerking bij OSINT) zal de CTIVD, in dialoog met de diensten, inzetten op de totstandkoming van een werkbaar tijdelijk toetsingskader dat door de diensten wordt vertaald in beleid, procedures en werkinstructies. In dit tijdelijke toetsingskader moet onder meer aandacht zijn voor de inrichting van een voorafgaande toets op de bepalingen omtrent gegevensverwerking, het criterium van stelselmatigheid bij openbronnenonderzoek, het houden van aantekening en de omgang met bronnen waarvan de herkomst en juistheid van de gegevens niet goed is vast te stellen.

Tot slot

OSINT vindt niet exclusief plaats binnen het domein van de inlichtingen- en veiligheidsdiensten, maar ook elders in het nationale veiligheidsdomein (bijvoorbeeld bij de NCTV) en daarbuiten (onder meer bij andere overheden). Dit rapport stelt vast dat OSINT zich in de loop der jaren verder heeft ontwikkeld en daarbij tools kunnen worden gebruikt die tegelijkertijd honderden bronnen raadplegen en waarvan de resultaten snel, overzichtelijk en in onderlinge samenhang worden weergegeven. Deze achterliggende bronnen kunnen locatiegegevens of gelekte gegevens bevatten. De verwerking van deze gegevens maakt een verdergaande inbreuk op de fundamentele rechten van betrokkenen dan bij OSINT via reguliere zoekmachines of op sociale mediadiensten.

De CTIVD verzoekt derhalve de ministers van Binnenlandse Zaken en Koninkrijksrelaties en van Defensie om dit rapport ook elders binnen de overheid onder de aandacht te brengen en bij toezending het Parlement te verzoeken het tevens ter kennis te brengen bij de Vaste Commissie voor Digitale Zaken van de Tweede Kamer.

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

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