

## Persbericht

---

Onderwerp  
CTIVD rapport nr. 74

Datum  
8 februari 2022

Op 8 februari 2022 publiceert de CTIVD het rapport 'automated OSINT: tools en bronnen voor openbronnenonderzoek'. Wanneer het verzamelen van een ieder toegankelijke gegevens geautomatiseerd plaatsvindt met behulp van specialistische software of webapplicaties ('tools'), is er sprake van 'automated OSINT'. Deze tools bevatten zoekfuncties en netwerkanalysefuncties, waarbij een grote diversiteit aan bronnen op een gebruikersvriendelijke manier kan worden geraadpleegd. In één zoekslag zijn tot wel honderden bronnen tegelijkertijd te raadplegen, waaronder locatiegegevens van de mobiele apparaten van personen en gelekte gegevens van gebruikers van sociale mediadiensten.

OSINT is nadrukkelijk niet meer alleen het 'naslaan' van telefoonboeken of zoeken van gegevens op internet via een zoekmachine. Het onderhavige onderzoek weerspiegelt het volgende: met automated OSINT kunnen honderden bronnen van diverse herkomst tegelijkertijd worden geraadpleegd, waaronder locatiegegevens en gelekte gegevens. Private bedrijven kunnen datasets samenvoegen als één raadpleegbare bron (een 'samengestelde dataset') met soms wel miljarden gegevens.

De locatiegegevens kunnen zijn gegenereerd via (internet)advertenties die worden getoond aan gebruikers van applicaties. Deze gegevens uit advertentiedata kunnen door de leveranciers van tools voor automated OSINT worden afgenomen bij datahandelaren ('data brokers') en via hun tools beschikbaar worden gesteld aan klanten, waaronder inlichtingen- en veiligheidsdiensten. In de Verenigde Staten heeft deze 'open source intelligence'-(OSINT) praktijk geleid tot vragen van Amerikaanse senatoren en tot (nog niet afgeronde) onderzoeken van Amerikaanse toezichthouders.

De CTIVD stelt in het rapport vast dat de huidige praktijk van automated OSINT een ernstiger privacy-inbreuk met zich meebrengt dan is voorzien bij de totstandkoming van de Wet op de inlichtingen- en veiligheidsdiensten 2017 (Wiv 2017). Daarom 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.

Voordat de tools in gebruik worden genomen moet in het kader van de verplichting tot een 'zorgvuldige gegevensverwerking' *voorafgaand* de werking en de achterliggende bronnen van de tools worden doorgrond. Uit het onderhavige onderzoek blijkt dat dit onvoldoende heeft plaatsgevonden. De CTIVD beveelt aan dat de beide diensten alsnog mitigerende maatregelen nemen om aan de algemene bepalingen in de Wiv 2017



omtrent gegevensverwerking te voldoen. Ook dienen de diensten hiervoor (bij voorkeur in gezamenlijkheid) een beleidskader te ontwikkelen. In dialoog met de diensten zal de CTIVD inzetten op de totstandkoming van een werkbaar tijdelijk toetsingskader met aandacht voor de inrichting van een voorafgaande toets op de bepalingen omtrent gegevensverwerking, het criterium van stelselmatigheid bij openbronnenonderzoek (de wet stelt extra waarborgen bij stelselmatig gebruik van open bronnen) en de omgang met bronnen waarvan de herkomst en juistheid van de gegevens niet goed is vast te stellen.

Ten slotte merkt de CTIVD op dat open source intelligence (OSINT) niet alleen plaatsvindt binnen het domein van de inlichtingen- en veiligheidsdiensten, maar ook elders in het nationale veiligheidsdomein (bijvoorbeeld bij de NCTV) en bij andere overheden. De CTIVD verzoekt derhalve de ministers van Binnenlandse Zaken en Koninkrijksrelaties en van Defensie om dit rapport elders binnen de overheid onder de aandacht te brengen en bij toezending het Parlement te verzoeken het tevens ter kennisneming te sturen aan de Vaste Commissie voor Digitale Zaken van de Tweede Kamer.