Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2021–2022

29 924 Toezichtsverslagen AIVD en MIVD

Nr. 223 **BRIEF VAN DE MINISTERS VAN BINNENLANDSE ZAKEN EN KONINKRIJKSRELATIES EN DEFENSIE**

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 8 februari 2022

Hierbij bieden wij u rapport nr. 74 van de Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (CTIVD) aan over automated OSINT[1]. Wij zijn de CTIVD erkentelijk voor het gedegen onderzoek, dat betrekking heeft op de periode 1 juli 2020 tot en met 31 maart 2021. In het rapport constateert de CTIVD geen onrechtmatigheden, wel één onzorgvuldigheid. Wij onderschrijven de conclusies van de CTIVD en nemen alle aanbevelingen over.

Algemeen

Op grond van de Wet op de inlichtingen- en veiligheidsdiensten (hierna: Wiv 2017) hebben de diensten de mogelijkheid om publiek toegankelijke gegevens te verzamelen en te verwerken. Het doen van openbronnenonderzoek wordt aangeduid met de term OSINT («open source intelligence»). Voorbeelden van openbronnen zijn Facebook- of Twitterpagina's die voor ieder persoon toegankelijk zijn. Waar een gewone burger vrijblijvend gebruik kan maken van deze open bronnen zijn de diensten gehouden aan een wettelijk kader waarop toezicht wordt uitgeoefend door de CTIVD. Openbronnenonderzoek betreft een algemene bevoegdheid, op grond van artikel 25 lid 1 onder a. Wiv 2017. Bij het uitvoeren van openbronnenonderzoek kunnen onderzoekers gebruik maken van specialistische software of webapplicaties. In dat geval is er sprake van automated OSINT. Het onderzoek van de CTIVD richt zich op de tools die door de diensten worden gebruikt en de bronnen die via deze tools geraadpleegd kunnen worden. Het onderzoek richt zich daarbij op de voorbereiding van een besluit tot aanschaf of verwerving van de automated OSINT tools en dus niet op de inzet van automated OSINT in concrete gevallen.

[1] Raadpleegbaar via www.tweedekamer.nl.

kst-29924-223
ISSN 0921 - 7371
's-Gravenhage 2022

Zoals de CTIVD in haar rapport constateert, heeft de praktijk van automated OSINT de afgelopen jaren een groei doorgemaakt. Het toenemend gebruik van automated OSINT is voor de diensten ook noodzakelijk. Deze noodzaak houdt allereerst verband met het subsidiariteitsvereiste: OSINT is een inlichtingenmiddel met een relatief geringe inbreuk op de privacy. Bovendien kan automated OSINT bijdragen aan het verifiëren van de betrouwbaarheid en juistheid van gegevens die verzameld zijn uit andere bronnen en daarmee een waarborg vormen.

Het doen van openbronnenonderzoek door de diensten is niet onbegrensd. Openbronnenonderzoek door de diensten maakt onderscheid tussen een niet- stelselmatige en stelselmatige inzet. Zodra bij het overnemen van gegevens uit open bronnen redelijkerwijs voorzienbaar is dat een min of meer volledig beeld van het privéleven van een persoon kan worden verkregen, is er sprake van een stelselmatige inzet. Op grond van artikel 38 Wiv 2017 dient in deze gevallen toestemming te worden gevraagd.

Conclusies en aanbevelingen

De CTIVD doet een aanbeveling aan de wetgever om een meer voorzienbare wettelijke grondslag voor automated OSINT met voldoende waarborgen te creëren. Op 1 mei 2020 is een onafhankelijke commissie ingesteld die de Wiv 2017 heeft geëvalueerd: de Evaluatiecommissie Wet op de inlichtingen- en veiligheidsdiensten 2017. Deze commissie heeft 20 januari 2021 haar evaluatierapport uitgebracht. Naar aanleiding van het evaluatierapport is een traject opgestart tot wijziging van de Wiv 2017. De aanbeveling voor een meer voorzienbare wettelijke grondslag voor automated OSINT wordt meegenomen in dit traject.

Het huidige artikel 38 Wiv 2017 is enkel van toepassing op het stelselmatig raadplegen van openbare bronnen, maar kent die waarborgen niet voor het stelselmatig raadplegen van commerciële bronnen (artikel 25 lid 1 sub b. Wiv 2017). Zowel open bronnen als commerciële bronnen kunnen echter in een OSINT-tool worden weergegeven. Vooruitlopend op het wetswijzigingstraject kiezen de diensten er daarom voor om de waarborgen behorende bij artikel 38 Wiv 2017 bovenwettelijk toe te passen indien redelijkerwijs voorzienbaar is dat via een OSINT-tool gegevens worden overgenomen uit commerciële bronnen die leiden tot een min of meer volledig beeld van iemands privéleven.

Bij de ontwikkeling of selectie en verwerving van een tool voor automated OSINT acht de CTIVD het in het kader van de zorgplicht voor zorgvuldige gegevensverwerking noodzakelijk dat de diensten zich op de hoogte stellen van de werking van de tool en de herkomst en aard van de bronnen die daarbij worden geraadpleegd. De CTIVD heeft op dit punt tekortkomingen geconstateerd ten aanzien van de reeds verworven tools. De CTIVD oordeelt dat de diensten «zo goed als mogelijk» de via deze tools te raadplegen bronnen moeten achterhalen en dat er wat dit betreft dus geen resultaatverplichting rust op de diensten. Ook constateert de CTIVD dat de diensten tijdens de selectie en verwerving van de tools wel voldoende rekening hebben gehouden met de operationele- en beveiligingsaspecten. De CTIVD doet een aanbeveling om in te zetten op een tijdelijk toetsingskader dat wordt omgezet in beleid, procedures en werkinstructies door de diensten. De diensten zullen het toetsingskader binnen afzienbare tijd opstellen en zullen de CTIVD hierbij betrekken.

Tot slot doet de CTIVD het verzoek om dit rapport ook elders binnen de overheid onder de aandacht te brengen nu OSINT niet exclusief plaatsvindt binnen het domein van de inlichtingen- en veiligheidsdiensten.

Omdat voor de inlichtingen- en veiligheidsdiensten een ander wettelijk kader voor verwerking van gegevens geldt dan voor de rest van de overheid zullen wij met de CTIVD in gesprek gaan hoe zo goed mogelijk uitvoering kan worden gegeven aan deze oproep.

De Minister van Binnenlandse Zaken en Koninkrijksrelaties,
H.G.J. Bruins Slot

De Minister van Defensie,
K.H. Ollongren