
CIVD
MIVD
JSCU
CTIVD
WIV
referendum 21 maart 2018
2017
AIVD
NSA
NCSC
TIB

INHOUD

REFERENDUM WIV 2017

Op 21 maart 2018 kunt u in het kader van een raadgevend referendum uw mening geven over de nieuwe Wet op de Inlichtingen- en Veiligheidsdiensten (WIV 2017). Deze wordt ook wel aangeduid als Sleepwet, hetgeen verwijst naar de uitbreiding van mogelijkheden om communicatieverkeer af te luisteren (door middel van bulkinterceptie) door de inlichtingendiensten (AIVD en MIVD). Dit is echter slechts één aspect van de WIV 2017.

Volgens de overheid draagt de WIV 2017 bij aan de nationale veiligheid en de effectiviteit van de inlichtingendiensten. Veel mensen denken hierbij in eerste instantie aan het voorkomen van terroristische aanslagen. De inlichtingendiensten richten zich echter niet alleen op (potentiële) terroristen, maar op veel meer mensen en zaken die vol gens de diensten een bedreiging zouden vormen voor de democratische rechtsorde. Een dreiging die echter niet altijd evident is.

Of de WIV 2017 daadwerkelijk op een positieve wijze zal bijdragen aan de het vergroten van de effectiviteit van betreffende inlichtingendiensten is nog maar de vraag. De AIVD en MIVD zijn weinig transparant over hun werkwijze en behaalde resultaten, en het toezicht alsmede de controle op de diensten is beperkt. Effectiviteit van het werk van de inlichtingendiensten valt dan ook moeilijk te beoordelen.

Buro Jansen & Janssen doet al ruim dertig jaar onderzoek naar inlichtingendiensten en heeft het nodige over het onderwerp gepubliceerd. Dit magazine bevat dan ook geen gedetailleerde analyse van alle wetsartikelen die opgenomen zijn in de WIV 2017. Een dergelijke exercitie kan nuttig zijn, maar levert slechts een beperkte bijdrage aan beantwoording van de vraag hoe de wet na invoering uiteindelijk zal uitpakken. We hebben gekozen voor een bredere benadering.

We proberen inzicht te geven in het functioneren van de Nederlandse inlichtingendiensten in zowel het heden als verleden. Hierbij komt een uiteenlopend aantal thema's aan bod, zoals de effectiviteit en toegevoegde waarde van de inlichtingendiensten, het toezicht en de controle erop, misstanden uit het verleden en lessen voor de toekomst, de risico's van in de wet opgenomen bevoegdheden (zoals hacken via derden en bulkinterceptie) en een vergelijking van de WIV 2017 met bestaande wetgeving in het buitenland.

Dit magazine is dan ook bedoeld als bijdrage voor het maken van een weloverwogen keuze bij het referendum.

Buro Jansen & Janssen

DE WIV IN HISTORISCH PERSPECTIEF

Buro Jansen & Janssen

Met invoering van de WIV 2017 worden de bevoegdheden van de inlichtingendiensten verder uitgebreid terwijl controlemogelijkheden en het toezicht op de werkwijze beperkt blijven.

De overheid wil de nieuwe Wet op de Inlichtingen- en Veiligheidsdiensten 2017 (WIV 2017) invoeren omdat de oude wet (WIV 2002) gemoderniseerd moet worden. Maar ook omdat de bevoegdheden in de 'oude' wet te beperkt zouden zijn voor de diensten. Bepaalde wetten zijn decennia oud en het is dan goed om deze aan te passen.

In verschillende sectoren, bijvoorbeeld zorg en welzijn, gaat modernisering vaak gepaard met bezuinigingen. Binnen het veiligheidsbeleid, waaronder ook de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) en Militaire Inlichtingen- en Veiligheidsdienst (MIVD) vallen, betekent modernisering doorgaans een uitbreiding van de bevoegdheden: de diensten krijgen meer middelen om mensen in de gaten te houden.

In de afgelopen decennia zijn bij wijzigingen van de WIV de bevoegdheden steeds verder uitgebreid. Vaak gaat het om een formalisering van de ontstane praktijk en werd er een wettelijke basis verschaft voor wat de diensten daarvoor (zonder wettelijke basis) toch al deden. Toezicht en controle op de diensten blijft bij iedere wetswijziging een problematisch onderwerp.

WIV 1987

Het werk van de inlichtingendiensten werd voor het eerst wettelijk geregeld met de invoering van de WIV in 1987. Daarvoor waren de taken en bevoegdheden van de diensten geregeld in een Koninklijk Besluit van 1949. De WIV 1987 was summier en bevatte een korte omschrijving van de taken van de Binnenlandse Veiligheidsdienst (BVD) en de Militaire Inlichtingendienst (MID), de voorlopers van de AIVD en MIVD, alsmede de Inlichtingendienst Buitenland (IDB) en hun samenwerking met het Openbaar Ministerie en politie.

De WIV 1987 raakte echter snel verouderd. De hierin opgenomen beperkte controlemogelijkheden door meerdere ministers en/of de Rechtbank Den Haag konden het ontsporen van de diensten niet voorkomen. Dit werd duidelijk uit een aantal schandalen. Zo kwam door een antimilitaristische actie van Onkruit aan het licht dat de inlichtingendiensten op grote schaal burgers bespiedden. De Nederlandse Staat werd hiervoor veroordeeld door het Europees Hof voor de Rechten van de Mens.

Eind 1993 bezweek de IDB aan allerlei interne schandalen, waarop de toenmalig minister-president Lubbers zelfs besloot een groot deel van de documenten van de IDB te vernietigen. Ten slotte bleek in 1994 tijdens een onderzoek uitgevoerd door de Parlementaire Enquêtecommissie Opsporingsmethoden (Commissie-

Van Traa) dat informatie van de inlichtingendiensten regelmatig en zonder wettelijke onderbouwing werd gebruikt voor opsporingsonderzoeken van politie en justitie.

WIV 2002

In 2002 werd de oude WIV vervangen door de huidige wet. De BVD werd vervangen door de AIVD, de MID door de MIVD. De taken van de opgeheven IDB werden overgeheveld naar de AIVD. In de nieuwe WIV 2002 werden de taken, bevoegdheden en werkzaamheden van de diensten uitgebreider beschreven.

Zo mochten de inlichtingendiensten het briefgeheim schenden (brieven openmaken) omdat ze toch ook al e-mails van burgers mochten lezen, waarmee een bestaande praktijk werd gelegaliseerd. Een verzoek voor het schenden van het briefgeheim moest nog wel worden voorgelegd aan de Rechtbank Den Haag.

Daarnaast werd de controle op het aftappen en afluisteren van burgers teruggebracht van meerdere ministers naar de verantwoordelijke minister (Binnenlandse Zaken voor de AIVD, Defensie voor de MIVD). Een deel van het toezicht op de diensten werd overgeheveld naar de nieuw opgezette Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (CTIVD).

De WIV 2002 werd op 7 februari 2002 bekrachtigd, maar de nieuwe bevoegdheden voor de inlichtingendiensten konden de moord op Pim Fortuyn (2002) niet voorkomen. Net als in de jaren '90 bleek dat de in de WIV 2002 opgenomen controlemogelijkheden te beperkt waren hetgeen leidde tot nieuwe misstappen door de diensten.

Voorbeelden hiervan zijn de moord op Theo van Gogh (de AIVD had de Hofstadgroep, waar de dader Mohammed B. deel van uitmaakte, wel degelijk in het vizier), de grote hoeveelheden onderschepte communicatie door de inlichtingendiensten (2009 – 2011), de door Edward Snowden onthulde 1,8 miljoen onderschepte telefoontjes die aan de Amerikaanse NSA zijn gegeven (2013) en het niet handelen na een tip van de Amerikaanse FBI en de Turkse overheid over Ibrahim el-Bakraoui die door Turkije werd uitgezet naar Nederland en zich later opblies op het Belgische vliegveld Zaventem (2016).

WIV 2017

In de vernieuwde WIV van 2017 worden de bevoegdheden van de diensten wederom uitgebreid. Tevens wordt de werkwijze van de AIVD en de MIVD expliciet vermeld. Denk hierbij aan het observeren en volgen van mensen, de inzet van agenten, het werven van informanten, het doorzoeken (fysiek inbreken) van huizen en andere locaties, hacken (digitaal inbreken), post openmaken, aftappen, afluisteren, communicatie en informatie over communicatie opvragen, bedrijven en stichtingen mogen opzetten en inzetten, DNA-profielen onderzoeken en toegang verlangen tot allerlei databanken. Het betreft hier grotendeels een formalisering van wat de diensten in de afgelopen jaren toch al deden.

Nieuw, of eigenlijk explicieter, omschrijft de WIV 2017 de bevoegdheid van het hacken van derden (toegang tot de gewenste computer verwerven via een computer of systeem van een andere (onverdachte) persoon of organisatie) en om communicatie (via kabels, satelliet en de ether) grootschalig af te tappen (bulkinterceptie). Dit laatste wordt in de wet 'onderzoeksopdrachtgericht onderzoek van communicatie' (OOG interceptie) genoemd. Dit is een breuk met het afluisteren en aftappen uit het verleden dat gericht was op individuen en organisaties/bedrijven.

Onderzoeksopdrachtgericht onderzoek is grofweg het aftappen/afluisteren van bijvoorbeeld bewoners van de Schilderswijk in Den Haag om mogelijk teruggekeerde Syriëgangers in de gaten te houden, of voor- en tegenstanders van Zwarte Piet. De WIV 2017 past in de historische trend: de bevoegdheden van de inlichtingendiensten worden wederom uitgebreid terwijl de controle en het toezicht gebrekkig blijven.

WIV: UITBREIDING OF PAAL EN PERK?

Tjepkema

De vraag is of de Wet op de Inlichtingen- en Veiligheidsdiensten moet blijven groeien naar de behoeften van de inlichtingendiensten, of juist een kader moet stellen.

Halverwege de jaren '50 van de vorige eeuw sloeg het 105 Verbindingsverkenningsbataljon zijn kamp op in Gorinchem. Met ruim tachtig kroegen een lustoord 'waar de meisjes niet schuw waren voor de wapenrok', aldus de toenmalige bataljonscommandant. Deze eenheid van de Koninklijke Landmacht was belast met het afluisteren en onderscheppen van berichten van radiozenders van het Sovjetleger en het peilen van zijn troepenbewegingen in het kader van de Koude Oorlog.

Zestig jaar later haalt de Nationale Signals Intelligence Organisatie (de NSO, een directe nazaat van het 105 Verbindingsverkenningsbataljon) de landelijke pers. In een maand tijd heeft de NSO 1,8 miljoen satelliettelefoontjes onderschept en metadata hierover doorgespeeld aan de Amerikaanse geheime dienst NSA, zo blijkt uit onthullingen door Edward Snowden.

RADIOSIGNAAL VOGELVRIJ

Er is blijkbaar nogal wat veranderd sinds de dagen dat een handjevol verbindingsofficieren het Gorkumse nachtleven onveilig maakte. De afgelopen zes decennia heeft communicatie een grote vlucht genomen en de bevoegdheden van de Nederlandse inlichtingendiensten groeien mee.

Radioverkeer neemt ten opzichte van communicatie via de kabel binnen de wetgeving een enigszins bijzondere positie in. Waar een kabel een begin en een eind heeft, straalt een radiozender alle kanten uit. Iemand die een radiozender gebruikt kan er in principe vanuit gaan dat iedereen met een geschikte ontvanger mee kan luisteren. Artikel 139c van het wetboek van strafrecht, waarin afluisteren strafbaar wordt gesteld, maakt dan ook een uitzondering voor het afluisteren van radiosignalen.

Ook de huidige Wet op de Inlichtingen- en Veiligheidsdiensten (WIV 2002) maakt hiervoor een uitzondering. Het plaatsen van een telefoontap mag alleen als er een concrete verdenking is. Radiosignalen daarentegen mogen ongericht en op grote schaal opgevangen worden. De vraag is of dit onderscheid nog van deze tijd is. Smartphones en satelliettelefoons maken immers ook gebruik van radiosignalen. Is in deze gevallen een bescherming van het telefoongeheim niet vanzelfsprekend?

Het telefoongeheim is samen met het briefgeheim vastgelegd in artikel 13 van de Nederlandse grondwet en mag alleen geschonden worden als daar bijzondere aanleiding voor is. Nu we steeds meer met elkaar communiceren, en een steeds groter deel van ons leven digitaal met elkaar delen, is de persoonlijke inbreuk van het afluisteren groter dan ooit. Ongeacht het medium.

Telkens wanneer de inlichtingendiensten iemand willen afluisteren moeten zij, en de verantwoordelijke minister, een afweging maken: staat deze inbreuk in verhouding tot het staatsbelang? In 2009 en 2011 brengt de Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (CTIVD) twee rapporten uit over de werkwijze van respectievelijk de Algemene Inlichtingen- en Veiligheidsdiensten (AIVD) en de Militaire Inlichtingen- en Veiligheidsdiensten (MIVD). Hieruit blijkt dat de motivering van de diensten regelmatig te kort schiet.

ONGESPECIFICEERDE VERZOEKEN

De diensten willen grote hoeveelheden onderschepte communicatie doorzoeken en moeten hiervoor formeel toestemming vragen aan de minister. Deze verzoeken zijn, volgens de CTIVD, onvoldoende gespecificeerd. Het is daardoor onmogelijk voor de toezichthouder om te controleren of het daadwerkelijk noodzakelijk was om tot afluisteren over te gaan, en of er geen andere mogelijkheden waren om dezelfde informatie te verkrijgen.

Het handelen van de diensten is daarmee volgens de CTIVD in strijd met de WIV 2002. De verantwoordelijke ministers wuiven het oordeel weg: het ligt niet aan de diensten, het ligt aan de wet. Nog geen tien jaar na invoering lijkt de WIV 2002 al te krap van opzet. In plaats van dat de diensten worden teruggefloten, moet de wet worden aangepast. Het zaadje voor de WIV 2017 is geplant.

Op welke schaal wordt er eigenlijk afgeluisterd? Precieze gegevens zijn niet bekend, maar de eerder genoemde 1,8 miljoen satelliettelefoontjes per maand geven wel een indicatie. In een wereldwijde markt van naar schatting 2 à 3 miljoen satelliettelefoon-abonnementen is dit een significant deel.

Daarnaast hebben de inlichtingendiensten sinds 2011 zo'n 17 miljoen euro geïnvesteerd in de aanschaf van speciale software voor de analyse van grote hoeveelheden communicatie. De aanbesteding voor dit project, Argo II genaamd, is waarschijnlijk gewonnen door het Israëlische bedrijf Nice Systems.
Het eerste contract loopt nog dit jaar af. De software is vooral gericht op het analyseren van IP-verkeer, oftewel internetverkeer dat grotendeels via de kabel loopt. Waarom de inlichtingendiensten deze analysecapaciteit nodig hebben, jaren voordat de bevoegdheid met de nieuwe WIV 2017 officieel ingaat, blijft onduidelijk.

ONDUIDELIJKHEDEN

Alhoewel de WIV 2017 het mogelijk maakt het telefoon- en internetverkeer van een hele stad of zelfs het hele land af te luisteren, is dat volgens de betrokken bewindslieden absoluut niet de bedoeling. Om dergelijke willekeur tegen te gaan wordt er voor het afluisteren een opdracht gedefinieerd, met toestemming van de minister en een speciale commissie

Hoe zo'n onderzoeksopdracht er precies uit gaat zien, is onduidelijk. In de memorie van toelichting voor de WIV 2017 spreekt men van een 'Geïntegreerde Aanwijzing inlichtingen- en veiligheidsdiensten' die een leidraad vormt 'waarin de regering in de richting van de diensten aangeeft wat noodzakelijk wordt geacht voor een veilig Nederland.'

Over wat voor soort zaken hebben we het dan? In de memorie van toelichting worden enkele voorbeelden genoemd. Zo wil men 18 maanden terug in de tijd kunnen zoeken naar de mogelijke oorsprong van een cyberaanval, of met terugwerkende kracht de bewegingen van terroristen volgen.

Met name bij een cyberaanval is het lastig te voorspellen hoe deze zal verlopen. Iedere met malware besmette computer kan immers door een hacker worden gebruikt om een volgend systeem aan te vallen. Ook de bewegingen van terroristen zijn lastig te volgen als je nog niet weet wie dat zijn. Hoeveel mensen moet men afluisteren en hoeveel computers moet men in de gaten houden om deze informatie te kunnen verzamelen?

De vraag is dus of de WIV moet blijven groeien naar de behoeften van de inlichtingendiensten, of juist een kader moet stellen? Hoe zullen de AIVD en MIVD opereren binnen de WIV 2017? Hoe zal de minister reageren als de wet opnieuw te krap van opzet blijkt? En hoe zal de WIV 2032 eruit komen te zien?

HACKEN DOOR DE INLICHTINGEN-DIENSTEN. VEILIG?

Jurre van Bergen

De WIV 2017 beoogt de veiligheid te vergroten, maar het hacken door de inlichtingendiensten leidt tot nieuwe veiligheidsrisico's voor de burger.

Het is de zomer van 2014. Op een kantoor in Zoetermeer rollen er allerlei tekens over het scherm van de hacker. Een analist ontvangt live camera beelden van wat een grauwe passage lijkt te zijn in een onbelangrijk gebouw nabij het Rode Plein in Moskou.

Maar niets is wat het lijkt. De AIVD heeft zojuist ingebroken bij de bekende Russische hackersclub Cozy Bear. De dienst ziet via camerabeelden personen naar binnen en buiten lopen, kan zo namen aan gezichten koppelen en de identiteit van de tot nu toe anonieme hackers achterhalen. De AIVD kan zelfs meekijken bij de operaties van Cozy Bear, bijvoorbeeld op het Ministerie van Buitenlandse Zaken, het Witte Huis en de Democratische Partij in de Verenigde Staten waarbij duizenden e-mails en documenten worden buitgemaakt.

Met dit verhaal komt de Volkskrant in januari van dit jaar naar buiten. Het geeft een inkijkje in de wereld van de inlichtingendiensten en de wijze waarop zij gebruik maken van haar hack bevoegdheden.

COLLATERAL DAMAGE VAN EEN HACK

In de WIV 2017 worden de hack bevoegdheden van de inlichtingendiensten deels uitgebreid en deels explicieter omschreven. Zo maakt de WIV 2017 hacken via derden (toegang tot de gewenste computer verwerven via een computer of systeem van een andere (onverdachte) persoon of organisatie) mogelijk. Los van de vraagtekens die hierbij geplaatst kunnen worden over de schendingen van de grondrechten van burgers, gaat het hacken door de overheid gepaard met aanzienlijke veiligheidsrisico's.

Hacken via derden vindt nu ook al plaats. Zo heeft de AIVD in het geval van Cozy Bear waarschijnlijk een signaal ontvangen met een IP-adres van het universiteitsgebouw in Moskou, waarna de dienst dit netwerk heeft gehackt om vervolgens mee te kijken met de Russische hackers. Met de invoering van de WIV 2017 valt echter te verwachten dat de inlichtingendiensten nog meer zullen hacken via derden.

Wat betekent dit? Laten we het voorbeeld nemen van Rob, een doelwit van de veiligheidsdiensten, die zo anoniem mogelijk het internet opgaat, niet rondloopt met een mobiele telefoon en thuis geen internetaansluiting heeft. Wel komen er vrienden over de vloer om wat bij te kletsen. Volgens de wet kan er op zulke momenten via een derde partij, in dit geval Ronald (een vriend van Rob) gehackt worden om vervolgens tot het doelwit te komen. Bijvoorbeeld door een microfoonfunctie in de mobiele telefoon van Ronald te installeren waardoor de diensten kunnen meeluisteren.

Bij het hacken mag de AIVD alle mogelijk middelen inzetten, zoals het installeren van malware, social engineering en zero-day kwetsbaarheden. Zero-days (nul dagen) zijn veiligheidslekken in software die nog niet bekend zijn bij de makers ervan en nog niet zijn gedicht. Terug naar het voorbeeld van Rob en Ronald.

ZERO-DAYS

De AIVD kan zelf software ontwikkelen om in te breken op een smartphone of tablet. Het lukt de dienst echter niet om de smartphone van Ronald te hacken (binnen te dringen). De dienst weet echter wel welke software en type telefoon Ronald gebruikt en gaat op zoek naar commerciële software om te hacken.

De AIVD kan zero-days op de vrije markt aanschaffen. Handel daarin is big business. Diverse bedrijven verkopen zero-days aan overheden en bedrijven en stimuleren zodoende het hacken van bijvoorbeeld smartphones. Wanneer makers van software niet op de hoogte worden gesteld van een veiligheidslek dan blijft een smartphone onveilig.

Handelaren in zero-days hebben echter geen enkel belang bij het melden van die lekken want zij verdienen eraan. Hierdoor wordt het ook voor cybercriminelen gemakkelijker om misbruik te maken van veiligheidslekken in software. Het vinden van beveiligingslekken is namelijk niet voorbehouden aan overheidsinstanties.

De reputatie van handelaren in zero-days is ook dubieus vanwege hun handel met autoritaire regimes die betrokken zijn bij mensenrechtenschendingen. Er zijn veel voorbeelden van activisten, advocaten en dissidenten die doelwit waren van een hack waarbij gebruik is gemaakt van zero-days.

Wat betekent dit voor Rob en Ronald? Niet alleen de AIVD heeft toegang tot de smartphone van Ronald, maar wellicht ook een cybercrimineel die bij dezelfde dubieuze handelaar shopt als de AIVD. Hacken via derden betekent dus dat ook derden last kunnen krijgen van cybercriminelen.

Ook veiligheidsdiensten zelf kunnen gehackt worden, hetgeen verregaande consequenties heeft. Dat dit geen hypothetisch risico is, bleek in 2016 toen de Amerikaanse inlichtingendienst National Security Agency (NSA) werd gehackt door een groep die zich de Shadow Brokers noemt. Zij maakten de zero-days die de NSA gebruikte voor haar eigen hacken openbaar. Een ieder kon nu gebruik maken van veiligheidslekken in software van laptops en servers.

SHADOW BROKERS WORM

Vervolgens ontwikkelden hackers op basis van de gevonden lekken een computerworm die via de beveiligingslekken binnen wist te dringen in netwerken en computers van bedrijven en instellingen. Met als gevolg dat computersystemen van diverse ziekenhuizen in Groot-Brittannië, containerterminals in Denemarken en parkeerbedrijven in Nederland gedeeltelijk tot compleet plat werden gelegd.

Het voorbeeld van de NSA rechtvaardigt de vraag of de Nederlandse inlichtingendiensten hun eigen beveiliging en de beveiliging van derden wel op orde hebben. De afgelopen jaren is regelmatig gebleken dat de digitale beveiliging van de Nederlandse overheid tekortschiet. Kan de AIVD dan ook voorkomen dat de dienst zelf gehackt wordt zodat de door haar gebruikte zero-days niet in handen vallen van cybercriminelen?

Volgens de WIV 2017 hoeven de inlichtingendiensten zero-days en andere kwetsbaarheden niet te melden. Dit is in strijd met het beleid van het Nationaal Cyber Security Centrum (NCSC) van het Ministerie van Justitie en Veiligheid dat de digitale weerbaarheid van Nederland juist wil vergroten. Het NCSC geeft zero-days zo snel mogelijk door aan makers van software zodat zij beveiligingslekken kunnen dichten en cybercriminelen geen kans krijgen.

Het onder de pet houden van zero-days door de AIVD staat dus haaks op het beleid van de NCSC. De WIV 2017 beoogt de veiligheid te vergroten, maar het hacken door de inlichtingendiensten leidt tot nieuwe veiligheidsrisico's voor de burger.

GEVAAR VOOR DE RECHTSORDE?

Buro Jansen & Janssen

De AIVD heeft een zeer ruime opvatting over personen en organisaties die een bedreiging zouden vormen voor de nationale veiligheid en democratische rechtsorde.

De AIVD houdt zich bezig met dreigingen tegen de Nederlandse staat en de democratische rechtsorde. Tijdens de Koude Oorlog, toen er sprake was van een duidelijk vijandbeeld, was het helder. Communisten vormden een bedreiging. Na de val van de Muur verlegde de AIVD haar werkterrein en werden ´bedreiging´ en ´democratische rechtsorde´ steeds ruimer gedefinieerd.

De gemiddelde Nederlander denkt bij het werk van inlichtingendiensten aan het voorkomen van terroristische aanslagen. De AIVD houdt zich echter ook bezig met een breed scala aan bewegingen, organisaties en individuen in Nederland. Denk bijvoorbeeld aan spanningen binnen de Turks-Koerdische gemeenschap, de discussie over de vestiging van asielzoekerscentra en demonstraties voor of tegen Zwarte Piet.

BIJZONDERE BEVOEGDHEDEN

De rapportages van de AIVD (door de dienst 'dreigingsproducten' genoemd) zijn veelal gebaseerd op informatie afkomstig van open bronnen op het internet, waaronder sociale media. Daarnaast kan de dienst ook bijzondere bevoegdheden inzetten om informatie over mensen in te winnen. Denk hierbij onder meer aan hacken, fysiek inbreken, afluisteren, het plaatsen van microfoons of camera's in huizen, observeren en de inzet van informanten.

De AIVD is geen opsporingsdienst en kan - in tegenstelling tot de politie - dus geen verdachten aanhouden en vervolgen. Burgers die de dienst in de gaten houdt, worden dus niet verdacht van een strafbaar feit. Aandacht van de AIVD en inzet van bijzondere bevoegdheden is echter wel ingrijpend voor burgers en kan alleen proportioneel zijn wanneer de doelgroep daadwerkelijk een bedreiging voor de rechtsorde vormt, zou je zeggen.

De AIVD schrijft in het jaarverslag 2016 dat de dienst rond de intocht van Sinterklaas van eind dat jaar in Maassluis twee dreigingsinschattingen, drie inlichtingenberichten en een ambtsbericht heeft opgesteld: 'De autoriteiten hebben hun maatregelen kunnen afstemmen op de onderkende dreiging.' De AIVD presenteert het in haar jaarverslag als de normaalste zaak van de wereld dat zij voor- en tegenstanders van Zwarte Piet in de gaten houdt.

Het is de vraag of dit wel als vanzelfsprekend moet worden beschouwd. Waren de mensen die protesteerden dan zo gevaarlijk? Vormt een demonstratie een bedreiging voor de rechtsorde? Een bericht op Facebook? De AIVD beschouwt voor- en tegenstanders van Zwarte Piet als een bedreiging voor de democratie, maar maken die burgers niet slechts gebruik van hun democratische recht op vrijheid van meningsuiting en demonstratie? Zwarte Piet wordt door de AIVD nog in haar jaarverslag

'Hoeveel burgers in dit land die zich bezig houden met politieke activiteiten worden er in de gaten gehouden?'

vermeld. Over veel (vermeende) bedreigingen rapporteert zij echter niet. De aandacht van de dienst en de inzet van bijzondere bevoegdheden komt dan anderszins aan het licht. Zo werd in 2005 bekend dat een AIVD-agente binnen de Arabisch Europese Liga (AEL) was geïnfiltreerd. De AEL was bezig met het opzetten van een politieke partij en het is de vraag hoe dit een bedreiging kan vormen voor de democratie.

In de afgelopen jaren kwam ook aan het licht dat studenten door de AIVD benaderd werden om informatie te verschaffen over de studentenprotesten en dat protestgroepen tegen de gaswinning in Groningen door de dienst in de gaten worden gehouden. Ook hier is het de vraag waarom deze groepen als een bedreiging voor de rechtsorde worden beschouwd. De AIVD hoeft hier geen verantwoording over af te leggen.

VEILIGHEIDSONDERZOEKEN

De informatie die de AIVD verzamelt, wordt ook gebruikt voor veiligheidsonderzoeken naar mensen die solliciteren op belangrijke of gevoelige functies bij de overheid en het bedrijfsleven. In 2016 verrichtte de AIVD 8.000 veiligheidsonderzoeken waarvan tien procent met een negatieve uitkomst. De consequenties van een veiligheidsonderzoek zijn groot, men kan een baan verliezen.
Ook nu is de vraag gerechtvaardigd wanneer iemand in de ogen van de AIVD een bedreiging vormt. Twee voorbeelden maken duidelijk welke informatie in een persoonsdossier kan belanden en wat de verstrekkende gevolgen daarvan kunnen zijn.

De Zeeuwse politiecommissaris Fup Goudswaard werd in 2008 ontslagen na een veiligheidsonderzoek door de AIVD. Volgens de dienst was hij chantabel omdat hij ooit een buitenechtelijke affaire had gehad. De AIVD was klaarblijkelijk diep in het privéleven van de commissaris gedoken, hetgeen de vraag oproept van hoeveel personen het privé leven nog meer in de gaten worden gehouden.

Evelien (fictieve naam) verloor haar baan als begeleider van passagiers op de luchthaven Schiphol omdat zij in het verleden actief was voor een actiegroep ter ondersteuning van politieke gevangenen in Spanje. Hoeveel burgers in dit land die zich bezig houden met politieke activiteiten worden er in de gaten gehouden? En waarom beschouwt de dienst een actiegroep, waarvan geen terroristische of gewelddadige activiteiten bekend zijn, als een bedreiging?

De AIVD heeft klaarblijkelijk een zeer ruime opvatting over personen en organisaties die een bedreiging zouden vormen voor de nationale veiligheid en democratische rechtsorde. Komen hierdoor de grondrechten van burgers niet in het geding?

REGERING STELT VERKEERDE PRIORITEITEN

Teun van Dongen

'Om het werk goed en effectief te kunnen blijven doen, moeten de diensten dan ook daar 'zijn' waar de informatie is.' Dit stelt de AIVD op haar website. De WIV 2017 richt zich derhalve vooral op de mogelijkheden van inlichtingendiensten om meer informatie te vergaren. De vraag echter is of dáár nu wel het probleem ligt. 'Zijn' de diensten dan niet daar waar de informatie zich bevindt?

Het Nederlands Juristen Comité voor de Mensenrechten heeft al in 2015 opgemerkt dat de regering met betrekking tot de nieuwe interceptiebevoegdheid die de WIV 2017 mogelijk maakt niet goed heeft uitgelegd 'waarom deze bevoegdheid noodzakelijk is, waarom de bestaande bevoegdheden niet in voldoende mate volstaan en welke (ernstige) problemen de voorgestelde bevoegdheid precies gaat oplossen'.

Dit is een belangrijke constatering, vooral gelet op het gegeven dat het bij het voorkomen van aanslagen veel vaker misgaat in de fasen die volgen op het vergaren van informatie. Politie- en inlichtingendiensten hebben doorgaans de informatie over verdachten in handen die ze nodig hebben, maar laten op andere momenten steken vallen.

BLUNDERS

Neem nu de aanslag in de kerk van het Normandische dorp Saint-Étienne-du-Rouvray in 2016. Een Franse agent in de regio was te weten gekomen dat twee jihadisten van plan waren om daar een bloedbad aan te richten, maar een van zijn superieuren was druk met andere dingen. Overige verantwoordelijke gezagsdragers waren met vakantie, waardoor de tip onbenut bleef.

Dit voorval staat niet op zichzelf. Een jaar later liep het in Manchester in Groot-Brittannië op een vergelijkbare manier mis. De Britse politie en de geheime dienst MI5 wisten al eerder dat de dader, Salman Abedi, een potentiële terrorist was, maar het overleg om de vervolgmaatregelen te bespreken stond pas gepland op 31 mei 2017, negen dagen na de aanslag.

Maar zelfs als waardevolle informatie niet blijft liggen, hebben terroristen nog kansen om door de mazen van het net te glippen. Zo kan het gebeuren dat de benodigde informatie beschikbaar is, maar dat de dreiging simpelweg verkeerd wordt ingeschat.

Zo wist de Duitse politie dat Anis Amri, de man die in december 2016 met een vrachtwagen op bezoekers van een kerstmarkt in Berlijn inreed, zich in extremistische kringen ophield en gepoogd had om aan wapens te komen. Tevens had hij zich aangeboden voor het plegen van een zelfmoordaanslag. Voor de Duitse politie was dit alles evenwel geen reden om hem als een serieuze bedreiging te zien.

Ook dit geval is niet uniek. Zo oordeelde de Deense veiligheidsdienst PET dat Omar Abdel Hamid El-Hussein niet gevaarlijk was, terwijl men ervoor was gewaarschuwd dat de man in de gevangenis was geradicaliseerd. Twee weken na zijn vrijlating in februari 2015 maakte hij twee dodelijke slachtoffers bij schietpartijen in het centrum van Kopenhagen.

En dan zijn er nog de gevallen waarin de uitvoering van de vervolgmaatregelen niet deugt. Mehdi Nemmouche stond onder politiesurveillance toen hij in 2014 een aanslag pleegde in het Joods Museum in Brussel, en de veroordeelde jihadist Omar H. werd door de AIVD in de gaten gehouden, maar slaagde er toch in om naar Syrië af te reizen. Het ernstigste geval is de meervoudige aanslag van november 2015 in Parijs. Deze werd voorafgegaan door een foutenfestival waar het laatste woord nog niet over is gezegd.

LESSEN LEREN

Het verijdelen van aanslagen is een proces dat meerdere fasen beslaat. Wat bovenstaande voorbeelden laten zien, is dat het probleem niet zozeer ligt in de fase van informatievergaring, waar de WIV 2017 over gaat. Met andere woorden, ook het overheidsoptreden rond aanslagen in andere landen maakt niet duidelijk 'welke (ernstige) problemen de voorgestelde bevoegdheid precies gaat oplossen'.

Maar als dat nu het geval is, zou het dan niet logischer zijn om de mogelijkheden voor het verbeteren van de Nederlandse terrorismebestrijding ergens anders te zoeken dan in uitbreiding van de bevoegdheden van de AIVD en de MIVD? Zou het bijvoorbeeld niet beter zijn om na te gaan wat er nog gedaan kan worden ter voorkoming van de fouten die aanslagen elders in Europa mogelijk hebben gemaakt?

Regeren is prioriteiten stellen, en het is nu eenmaal zo dat daar soms ongemakkelijke keuzes voor nodig zijn. Echter, met de WIV 2017 stelt de overheid verkeerde prioriteiten. Door lessen te trekken uit aanslagen in andere landen moet het mogelijk te zijn om maatregelen te bedenken die minder ingrijpend zijn en meer opleveren.

WAAR IS BULKINTERCEPTIE GOED VOOR?

Buro Jansen & Janssen

Volgens de overheid is bulkinterceptie noodzakelijk om aanslagen te voorkomen. Maar het middel kan het zicht van de inlichtingendiensten vertroebelen waardoor potentiële aanslagplegers door de mazen van het sleepnet glippen.

Het massaal aftappen van het internetverkeer, ook wel bulkinterceptie genoemd, is volgens de overheid noodzakelijk om de nationale veiligheid te vergroten en terroristische aanslagen te voorkomen. De in de WIV 2017 opgenomen bulkinterceptie geeft de diensten de mogelijkheid om grote hoeveelheden communicatie zonder selectie, dus van iedereen in een bepaalde stad of zelfs land, te verzamelen.

Deze taak wordt uitgevoerd door een gezamenlijke eenheid van de AIVD en de MIVD, de Joint Sigint Cyber Unit (JSCU). Of met de inzet van bulkinterceptie inderdaad aanslagen worden voorkomen, valt niet vast te stellen. Nederland heeft er immers nog geen ervaring mee. In Groot-Brittannië is wél onderzoek gedaan.

MR. ANDERSON

Het onderzoek van David Anderson naar bulkinterceptie door de Britse inlichtingendiensten MI5, MI6 en GCHQ maakt onderdeel uit van het rapport Report of the Bulk Powers review uit augustus 2016. Het onderzoek heeft niet alleen betrekking op bulkinterceptie in het kader van terrorismebestrijding. Het middel wordt in Groot-Brittannië namelijk breder ingezet en er is ook sprake van andere 'bulkbevoegdheden'.

Anderson's onderzoek berust op een analyse van dertien casussen uit de periode 2009 – 2016. Vijf hiervan hebben betrekking op contraterrorisme-operaties. Het totaal aantal gevallen waarin bulkinterceptie werd toegepast, wordt in het rapport niet vermeld. De casussen zijn door de inlichtingendiensten geselecteerd. Het is niet bekend hoe het aantal succesvolle casussen zich verhoudt tot het aantal niet-succesvolle. Het rapport kent hiermee dus z'n tekortkomingen.

Er is wel een opvallende rode draad waar te nemen in de vijf casussen draaiend om contraterrorisme-operaties. Bulkinterceptie blijkt door Britse diensten vooral te zijn toegepast in gevallen waarbij de uiteindelijke verdachten al deel uitmaakten van een bestaand terrorismenetwerk of contact hadden met bij de diensten bekende leden van terreurorganisaties. Men zou dan ook kunnen stellen dat de inlichtingendiensten de verdachten sowieso al in het vizier hadden.

BEKENDE VERDACHTEN

Een van de casussen heeft betrekking op de arrestatie van twaalf personen in april 2009 die verdacht werden van voorbereiding van een aanslag op een winkelcentrum in Manchester. De verdachten stonden in direct contact met een lid van de terreurorganisatie Al Qaida in Pakistan. De diensten beschouwen de inzet van bulkinterceptie in deze casus als succesvol, onder meer omdat hiermee een e-mailadres van een verdachte kon worden geïdentificeerd. De verdachten werden

overigens vrijgesproken omdat er geen bewijs was dat ze daadwerkelijk een aanslag wilden plegen; ze hadden er slechts over gefantaseerd.

Een andere casus betreft de arrestatie en de veroordeling in 2011 van Rajib Karim die werkzaam was bij British Airways en toegang had tot vliegtuigen. Hij en zijn broer waren in Bangladesh lid geweest van de verboden organisatie Jammat-ul Mujahideen Bangladesh. Karim emigreerde naar Engeland, zijn broer sloot zich in Jemen aan bij het netwerk van de Amerikaanse prediker Anwar Al-Awlaki die zijn volgers opriep om aanslagen te plegen. Al-Awlaki werd sinds 2009 gezocht als terreurverdachte en in 2011 door een Amerikaanse drone gedood.

Ook bij deze casus is het de vraag of bulkinterceptie noodzakelijk was omdat Karim al in direct contact stond met een netwerk bestaande uit bij de dienst bekende terreurverdachten.

De Britse inlichtingendiensten beschouwen de inzet van bulkinterceptie als nuttig, een conclusie die door onderzoeker Anderson wordt overgenomen. Het is echter de vraag of bulkinterceptie in de door Anderson beschreven casussen een noodzakelijk middel was. De Britse diensten hebben immers al gerichte bevoegdheden om specifieke mensen en derden actief binnen terreurnetwerken in de gaten te houden.

ONZICHTBAAR BINNEN HET NETWERK

Heel veel data verzamelen heeft namelijk ook nadelen die in het onderzoek niet behandeld worden. Het kan eraan bijdragen dat de diensten hun zicht op personen binnen diezelfde netwerken verliezen. Dit werd in 2017 pijnlijk duidelijk.

Salman Abedi blies zichzelf op 22 mei 2017 tijdens een popconcert in Manchester op. Tweeëntwintig mensen verloren hierbij het. Abedi bleek al sinds 2014 in beeld te zijn bij MI5 als zijnde bekende van een persoon die door de dienst in de gaten werd gehouden.

In oktober 2015 kwam Abedi opnieuw in beeld als een bekende van een IS-aanhanger in Libië. Tevens was het bij de Britse inlichtingendiensten bekend dat Abedi extremistische denkbeelden deelde. Hij reisde naar Turkije en Libië en kon vervolgens zonder problemen terugkeren naar Groot-Brittannië. Onderzoek naar de aanslag in Manchester maakte duidelijk dat de bom die hij tot ontploffing bracht door hem zelf was vervaardigd in zijn keuken met behulp van films op YouTube.

De zaak roept vragen op. Abedi opereerde immers binnen een bij de diensten bekend netwerk van terrorismeverdachten. Het valt moeilijk te begrijpen dat de Britse inlichtingendiensten niet tijdig ingrepen. Natuurlijk is terrorismebestrijding mensenwerk en het valt nooit uit te sluiten dat de diensten iets missen, maar de focus op bulkinterceptie maakt het voorbeeld van Abedi echter bijzonder wrang. De diensten richtten zich met inzet van het middel op grote delen van de Britse samenleving, terwijl er binnen een bij hen bekend terreurnetwerk een aanslag werd voorbereid.

ZICHT ONTNOMEN

Met de WIV 2017 krijgen nu ook de Nederlandse inlichtingendiensten de bevoegdheid om bulkinterceptie in te zetten als opsporingsmiddel. De AIVD stelt dat het jihadistische netwerken en Syriëgangers in de gaten heeft. Volgens AIVD-directeur Rob Bertholee heeft de dienst daarnaast in zes jaar tijd vier aanslagen weten te voorkomen.

Er heeft geen aanslag plaatsgevonden in Nederland dus de conclusie zou kunnen zijn dat de diensten de netwerken van terreurverdachten en de mensen die daarmee contact leggen al voldoende in de gaten houden. De AIVD wil echter het sleepnet verder uitwerpen om zo meer informatie over nog meer personen te verzamelen en op zoek te gaan naar nieuwe potentiële terroristen.

Of de extra bevoegdheid tot bulkinterceptie de effectiviteit van de diensten zal bevorderen, is niet in te schatten. De Britse ervaringen geven aanleiding tot scepsis. Wanneer - zoals in Groot-Brittannië - bulkinterceptie voornamelijk leidt tot personen die reeds onderdeel uitmaken van verdachte terrorismenetwerken, is het de vraag wat bulkinterceptie toevoegt aan de reeds bestaande bevoegdheden.

Vertroebelt de focus op bulkdata niet juist het zicht van de AIVD/MIVD in hun speurtocht naar potentiële aanslagplegers?

RESULTAAT INZET INLICHTINGEN-DIENSTEN ONBEKEND

Buro Jansen & Janssen

Het gebrek aan transparantie van de AIVD en MIVD maakt een analyse van de effectiviteit en toegevoegde waarde van hun bijdragen aan de nationale veiligheid onmogelijk.

Nederland kent twee inlichtingendiensten. De Algemene Inlichtingen- en Veiligheidsdienst (AIVD) brengt politiek maatschappelijke ontwikkelingen en bedreigingen in kaart en waarschuwt voor bedreigingen en risico's. Volgens haar jaarverslag van 2016 produceerde de dienst 152 ambtsberichten, 457 inlichtingenrapporten en 118 dreigingsproducten. Het jaarverslag specificeert niet over welke onderwerpen is gerapporteerd.

De Militaire Inlichtingen- en Veiligheidsdienst (MIVD) levert informatie 'om de verdedigingstaken van Defensie goed voor te bereiden, bij besluiten over deelname aan operaties, en tijdens operaties'. Volgens het jaarverslag heeft de dienst in 2016 dreigingsanalyses en inlichtingenproducten aan verschillende Ministeries gestuurd, maar er wordt niet vermeld om hoeveel analyses het gaat en waar deze over gaan. De analyses en rapportages van zowel de MIVD als de AIVD zijn niet openbaar.

OPENBARE BRONNEN

De informatie die de AIVD en de MIVD gebruiken voor hun rapporten is vooral afkomstig uit openbare bronnen zoals mediaberichtgeving. De MIVD stelt in haar jaarverslag zelfs expliciet dat het zoveel mogelijk gebruik maakt van openbare bronnen. Dit roept de vraag op in hoeverre de rapporten en analyses van de diensten de kennis van een gemiddelde krantenlezer overstijgen. De MIVD lijkt dit deels te onderschrijven: 'Niet elke analyse kan met de gewenste diepgang worden geleverd.'

Welke consequenties dit gebrek aan diepgang heeft, maakt de dienst niet duidelijk. Wel blijft de MIVD in haar jaarverslag steken bij een zeer algemene en vrijblijvende opmerking: 'Het is bijvoorbeeld belangrijk dat de militairen in het veld op tijd weten dat de tegenstander een aanslag voorbereidt.' De MIVD maakt echter niet bekend hoe vaak ze een aanslag in het vizier heeft gehad en wist te voorkomen.

De diensten hebben echter wel veel pretenties. De AIVD schrijft dat het haar taak is 'om dreigingen, risico's en internationale politieke ontwikkelingen, die anderen niet kunnen zien en die grote gevolgen kunnen hebben voor de belangen van de Nederlandse staat, als eerste te onderkennen en te duiden.' Het is echter de vraag in hoeverre de AIVD daadwerkelijk risico's als eerste onderkent en duidt want de claim wordt verder niet onderbouwd. In de paragraaf 'toegevoegde waarde AIVD' wordt slechts vermeld dat er een 'meerjarenvisiedocument' is geschreven. Het MIVD-jaarverslag 2016 bevat geen paragraaf over haar toegevoegde waarde.

De AIVD en MIVD brengen dus bedreigingen in kaart, maar het is niet altijd op voorhand duidelijk waar die

uit bestaan. Zo houden beide diensten zich volgens hun jaarverslagen bezig met de politiek-economische situatie in Venezuela. De MIVD schrijft dat ze hiervoor inlichtingen en achtergrondinformatie verzamelt uit openbare bronnen. De AIVD schrijft dat Venezuela in 2016 door een diepe crisis gaat die een negatief effect heeft op de Nederlandse Antillen. Het wordt echter niet duidelijk om wat voor effect het gaat en op welke wijze de rapportages en inlichtingen van de diensten hebben bijgedragen aan de veiligheid van de Nederlandse staat.

VLIEGRAMP MH17

Het gebrek aan transparantie van de AIVD en MIVD werd pregnant zichtbaar naar aanleiding van de ramp met de MH17 in Oekraïne in 2014. Wat hebben de diensten gedaan en hadden zij deze ramp kunnen of moeten zien te voorkomen? Uit de jaarverslagen blijkt dat beide diensten de situatie in de regio volgen, maar het blijft onduidelijk waar dit toe heeft geleid.

De Commissie Toezicht Inlichtingen- en Veiligheidsdiensten (CTIVD) boog zich over de kwestie en oordeelde in april 2015 dat de diensten geen kennis hadden over de aanwezigheid van 'militaire middelen, mogelijkheden en intentie' in het gebied om burgervliegtuigen mee uit de lucht te schieten. Wel was de CTIVD van mening dat de 'de veiligheid van vliegroutes in het buitenland' tot de taken van de AIVD behoort.

Enkele maanden later stelde de onderzoekscommissie naar het neerstorten van MH17 echter vast dat de MIVD wel degelijk kennis had over de aanwezigheid van zware wapens in het gebied in het noorden van Oekraïne. Hoewel twee onderzoekscommissies verschillende conclusies trokken, blijft de vraag welke dreigingsproducten de AIVD en de MIVD over Oekraïne hebben opgesteld en wat hiervan de meerwaarde was.

RUSSISCHE BEÏNVLOEDING

De AIVD houdt zich ook bezig met digitale dreiging, de veiligheid van overheidsinformatie en 'beïnvloedingsoperaties'. Volgens het jaarverslag 2016 was Nederland herhaaldelijk doelwit van hardnekkige omvangrijke spionage-aanvallen die door de AIVD vroegtijdig zijn onderkend. De dienst maakt niet concreet wat voor inspanningen er zijn verricht en hoeveel aanvallen het hier betreft.

Digitale bedreigingen worden door de AIVD in verband gebracht met Rusland. Onder de kop 'Rusland grijpt terug op beïnvloedingsoperaties' verwijst de dienst hier in haar jaarverslag 2016 reeds naar. Eind 2017 stelt minister Ollongren hier zelfs een brief over op voor de leden van de Tweede Kamer waarin ze claimt dat Rusland zich zou bemoeien met Nederlandse interne aangelegenheden zoals de verkiezingen van 2017.

De directeur van de AIVD, Bertholee, hierover: 'Ik denk dat wel gepoogd is om de kiezers mogelijk in een verkeerde richting te duwen door berichten te verspreiden die niet of slechts ten dele waar zijn.' De AIVD suggereert dus dat Rusland de Nederlandse verkiezingen heeft proberen te beïnvloeden, maar levert hiervoor geen concreet bewijs.

WORDEN AANSLAGEN VOORKOMEN?

De strijd tegen terrorisme is een topprioriteit van de inlichtingendiensten en het is voor de reputatie van de AIVD positief dat zij successen hieromtrent kan melden. Zo vertelde AIVD-directeur Bertholee in het tv-programma College Tour (21-03-18) dat de AIVD in zes jaar tijd vier terroristische aanslagen heeft weten te voorkomen.

Het is echter bekend dat een van de vier aanslagen is voorkomen dankzij een tip van een burger. Over de drie andere voorvallen levert de AIVD geen informatie. De dienst zegt wel dat zij in 2016 maar liefst 5.400 tips heeft binnengekregen, waarvan 238 tot nader onderzoek hebben geleid, zonder toe te lichten welke resultaten de onderzoeken hebben opgeleverd.

Het is om die reden wrang dat de AIVD in haar jaarverslag 2016 geen melding maakt van een tip van de Amerikaanse FBI over Ibrahim el-Bakraoui, een Belg die door Turkije werd uitgezet naar Nederland en die zichzelf op 22 maart 2016 opblies in een hal van het Belgische vliegveld Zaventem.

TOEZICHT OP DE INLICHTINGEN- EN VEILIGHEIDSDIENSTEN

Het toezicht op de AIVD en MIVD wordt uitgevoerd door de Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (CTIVD). Daarnaast is er een parlementaire Commissie voor de Inlichtingen- en Veiligheidsdiensten (CIVD), in de volksmond ook wel de commissie Stiekem genoemd. En tot slot is in de WIV een nieuwe commissie opgenomen: de Toetsingscommissie Inzet Bevoegdheden (TIB).

CTIVD: TOEZICHT ZONDER GEVOLGEN?

Buro Jansen & Janssen

Toezicht en controle op de AIVD en MIVD is in de loop der jaren mondjesmaat toegenomen. Tot 2002 waren de verantwoordelijke ministers, soms aangevuld met andere ministers of de Rechtbank Den Haag, hiervoor verantwoordelijk. Daarna veranderde dit met de invoering van de Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (CTIVD).

De CTIVD beoordeelt achteraf of de AIVD en de MIVD zich aan de regels en wetgeving hebben gehouden en geeft adviezen. De verantwoordelijke ministers kunnen de aanbevelingen van het CTIVD naast zich neerleggen. De toezichthouder heeft inmiddels 55 rapporten gepubliceerd. In 2016 heeft zij vijf rapportages afgerond, waaronder bijvoorbeeld een rapport over de afluisterbevoegdheid van de MIVD en een rapport over de invulling van criteria voor samenwerking met buitenlandse diensten.

De CTIVD probeert kwalitatief goed onderzoek te doen. Hoe effectief het toezicht is, blijft echter onduidelijk. In haar laatste jaarverslag over 2016 neemt de CTIVD voor het eerst sinds haar bestaan een hoofdstuk op over de effectiviteit van toezicht. De commissie stelt dat de verantwoordelijke ministers doorgaans toezeggen de aanbevelingen van de CITVD over te nemen. Of dit ook daadwerkelijk het geval is, onderbouwt de commissie echter niet met concrete voorbeelden. De commissie houdt zelf niet bij in hoeverre de aanbevelingen daadwerkelijk zijn doorgevoerd.

Ook vermeldt de CTIVD dat 'de AIVD of de MIVD soms reeds tijdens een onderzoek een aanvang nemen met het aanpassen van beleid en werkwijzen.' De commissie geeft hiervan twee voorbeelden: rapport 50 over de bijdrage van de MIVD aan targeting (augustus 2016) en rapport 51 over de uitvoering van de notificatieplicht (december 2016). Ook hier verzuimt de commissie om aan te geven of de aanpassingen niet alleen in gang zijn gezet, maar ook daadwerkelijk zijn doorgevoerd.

Opvallend is dan ook de laatste paragraaf van het hoofdstuk over effectiviteit, 'de implementatie van aanbevelingen'. De CTIVD schrijft dat zij voor de derde keer onderzoek doet naar de notificatieplicht door de AIVD en dat de commissie zelf niet controleert in hoeverre haar aanbevelingen worden nageleefd.

Het is zeer de vraag hoe effectief het toezicht in werkelijkheid is en in hoeverre aanbevelingen leiden tot aanpassingen in het beleid met betrekking tot de werkwijze van de diensten. De CTIVD lijkt zich na veertien jaar ook af te vragen hoe effectief haar eigen werk eigenlijk is. Volgens het jaarverslag bezint de commissie zich om 'de effectiviteit van haar toezicht te bevorderen'.

CIVD: ONNODIG STIEKEM?

Buro Jansen & Janssen

'De commissie vergadert onder strikte geheimhouding, maar brengt summier verslag uit aan de Kamer.'

De Commissie voor de Inlichtingen- en Veiligheidsdiensten (CIVD), in de volksmond ook wel de commissie Stiekem genoemd, bestaat sinds 1952. In de commissie hebben de fractievoorzitters van de grootste partijen zitting. Op dit moment bestaat de CIVD uit vijf fractievoorzitters, drie van de coalitiepartijen (VVD, CDA, D66) en twee van oppositiepartijen (PVV en GL).
De commissie vergadert onder strikte geheimhouding, maar brengt summier verslag uit aan de Kamer.

Het functioneren van de CIVD staat al jarenlang ter discussie. Toenmalig commissievoorzitter Van Thijn zat in de jaren '70 regelmatig alleen te vergaderen met ministers en ambtenaren. Naar verluidt zaten sommige fractievoorzitters, die wel kwamen opdagen, te slapen of hadden zij de stukken niet gelezen. Het is niet bekend of het met de vergaderdiscipline van de commissie nog steeds zo schrijnend gesteld is. Wel is bekend dat de helft van de leden in 2016 niet op de vergaderingen aanwezig was.

De discussie binnen de CIVD is weinig diepgravend hetgeen door meerdere betrokkenen bevestigd wordt. Ook voormalig minister Remkes (Binnenlandse Zaken) vond het debat wat oppervlakkig tijdens zijn ministerschap (2002 – 2007). Fractievoorzitters hebben vele prioriteiten en niet de specialistische kennis om de juiste vragen te kunnen stellen. De geringe voorbereidingstijd is hier debet aan. Documenten worden nauwelijks ingezien omdat deze na aanvraag in een aparte kamer en onder begeleiding voorafgaande de vergadering moeten worden gelezen.
Het gebrek aan diepgang blijkt tevens uit de geringe tijdsduur van agendering. Zo duurde de bespreking van het zeven pagina's tellende jaarverslag over 2013 welgeteld elf minuten. De rapporten van toezichthouder CTIVD worden niet of nauwelijks besproken. De CTIVD-rapporten zijn overigens openbaar en kunnen dus ook besproken worden in de Vaste Kamercommissie voor Binnenlandse Zaken en Defensie. Dit gebeurt echter zelden. Van parlementair toezicht op de diensten is dan ook nauwelijks sprake.

Geheimhouding is op zichzelf een problematisch aspect van de commissie Stiekem. De fractievoorzitters mogen de informatie die door de diensten in de commissie gedeeld wordt niet in het parlement of met hun fractiespecialisten bespreken. Dit verzwakt vanzelfsprekend de parlementaire controle.

Het is echter de vraag in hoeverre die geheimhouding altijd noodzakelijk is, of dat er vooral sprake is van veel onnodige geheimhouding. Informatie over beleidsmatige kwesties vereist bijvoorbeeld veel minder geheimhouding dan nu het geval is. Illustratief voor de geheimhoudingsreflex van de commissie Stiekem is het rapport dat ze liet opstellen over het verbeteren van de commissie (Naar een sterker functionerende CIVD). Het rapport zelf bleef namelijk geheim en ook de bespreking hiervan in 2016 was niet openbaar.

TIB: ONAFHANKELIJKHEID IN HET GEDING?

Buro Jansen & Janssen

In de WIV 2017 heeft de wetgever een nieuwe commissie in het leven geroepen: de Toetsingscommissie Inzet Bevoegdheden (TIB). De TIB toetst of de besluiten van de minister over de inzet van bevoegdheden rechtmatig zijn, bijvoorbeeld een besluit om over te gaan tot bulkinterceptie of hacken. Anders dan de reeds bestaande Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten(CTIVD) toetst de TIB de inzet van bevoegdheden vooraf.

De benoemingsprocedure voor de TIB wordt in de WIV 2017 omschreven. De commissie bestaat uit een voorzitter en twee leden, waarvan één lid over technische deskundigheid dient te beschikken. De Nationaal Ombudsman en de hoogste rechters bevelen gezamenlijk voor elke functie drie potentiële kandidaten aan. Daarna draagt de Tweede Kamer per functie drie kandidaten voor aan de minister van Binnenlandse Zaken: voor het voorzitterschap, het algemene lid en voor de technisch expert.

De minister maakt hieruit vervolgens een keuze en benoemt de commissieleden. Leden van de TIB mogen volgens de WIV 2017 geen 'betrekkingen uitoefenen' die nadelig kunnen zijn voor de vervulling van hun commissiefunctie of die hun onpartijdigheid en onafhankelijkheid schaadt. De TIB-leden worden hiervoor aan een veiligheidsonderzoek van de AIVD onderworpen.

Op het eerste gezicht lijkt dit een zorgvuldige procedure, maar de praktijk wees anders uit. De aanbeveling van de Ombudsman en rechters aan de Tweede Kamer bleek onvolledig. Zij stelden voor de functie van technisch expert twee in plaats van drie kandidaten voor. De keuze is gevallen op voormalig AIVD-medewerker Ronald Prins. Hij is tevens mede-eigenaar van een technologie investeringsfonds dat zich onder meer richt op big data en gegevensverwerking, en oprichter van Fox-IT, een cyber security bedrijf dat veel opdrachten ontvangt van de AIVD.

De benoeming van Prins is zeer opmerkelijk te noemen. Hij is oud-AIVD'er en als adviseur verbonden aan een bedrijf dat klant is van de AIVD. Het lijkt evident dat zijn onpartijdigheid en onafhankelijkheid, en ook die van de TIB, hiermee in het geding is. De minister en leden van de Tweede Kamer hebben hier echter geen problemen mee.

De TIB kan voorkomen dat bevoegdheden verkeerd/onrechtmatig worden ingezet. Het is echter de vraag in hoeverre de invoering van deze nieuwe commissie daadwerkelijk zal leiden tot een verbetering van het toezicht en de controle op de diensten. Het verloop van de benoemingsprocedure kan wellicht als valse start worden afgedaan, maar geeft weinig aanleiding om de toekomst met vertrouwen tegemoet te zien.

BVD: LESSEN UIT HET VERLEDEN

Jos van Dijk auteur van 'Ondanks hun dappere verzet', 2016

Kunnen we er op vertrouwen dat een geheime dienst die geen afstand heeft gedaan van een dubieus verleden in de huidige praktijk wél de nodige zorgvuldigheid zal betrachten?

Ondanks veel gemopper over allerlei zaken hebben de meeste Nederlanders in het algemeen nog wel vertrouwen in wat de overheid namens ons doet of nalaat. De rechtsstaat is stevig verankerd in de samenleving. Wetten bieden de burgers in principe bescherming tegen onrecht, onveiligheid, machtsmisbruik en willekeur.

Maar soms pakt de praktijk voor een individu of groep anders uit en dat doet afbreuk aan het vertrouwen. Denk aan Groningen en de aardbevingen. Zoiets vraagt van de overheid een adequate reactie om groeiend wantrouwen te voorkomen. Arrogantie van de macht maakt de problemen alleen maar groter.

Wetgeving die het handelen van geheime diensten regelt, is bijzonder kwetsbaar voor de vertrouwensrelatie met de burgers. De diensten moeten in het geheim opereren omdat ze anders hun opdracht, bescherming van de democratie, niet kunnen uitvoeren. Dat vraagt om extra waarborgen en controle-instrumenten om te voorkomen dat ons vertrouwen in de praktijk wordt geschaad.

Eens te meer geldt hier: vertrouwen is goed, controle is beter. Bij de beoordeling van de WIV 2017 gaat het dus niet alleen om de vraag of de letter van de wet ons vertrouwen waard is, maar ook of we de uitvoering van de wet met vertrouwen tegemoet kunnen zien.

DE KOUDE OORLOG

De huidige AIVD is een voortzetting van de oude Binnenlandse Veiligheidsdienst (BVD). De dienst werd in de periode van de Koude Oorlog gedomineerd door een hardnekkige anticommunistische tunnelvisie die zich binnenslands uitte in de vorm van inmenging en ontregeling van de communistische partij en daaraan gelieerde organisaties.

De BVD heeft zijn officiële opdracht, het verzamelen van inlichtingen over mogelijke bedreigingen van de democratie, altijd bijzonder ruim geïnterpreteerd. Tot tweemaal toe heeft de dienst een nep-politieke partij opgericht en gefinancierd om verwarring en verdeeldheid te zaaien. In de verantwoording naar de politiek was de dienst nogal selectief. Sommige geheime operaties waren alleen bekend bij de verantwoordelijke minister en bij de buitenlandse diensten waarmee de BVD samenwerkte.

De BVD heeft veel werk gemaakt van het vastleggen van gedetailleerde gegevens van burgers, niet zelden op

'Tot tweemaal toe heeft de dienst een nep-politieke partij opgericht en gefinancierd om verwarring en verdeeldheid te zaaien.'

basis van geruchten, valse aantijgingen of onschuldige uitingen zoals verkiezingsposters of het lezen van het voormalige communistische dagblad De Waarheid.

De geschiedschrijver van de BVD, Dick Engelen, schat dat er in de cartotheken van de geheime dienst honderdduizenden namen zijn geregistreerd die werden gebruikt om mensen af te wijzen voor willekeurige banen, niet alleen bij de overheid, maar ook in het onderwijs en bij de universiteit. Artiesten die hun medewerking gaven aan CPN-bijeenkomsten werden op gezag van de BVD geboycot. Kunstenaars zoals mimespeler Rob van Reijn en hoboïst Haakon Stotijn kregen geen visum voor de Verenigde Staten.

KEIHARDE CHANTAGE

Bij het werven van informanten schrok de BVD niet terug voor keiharde chantage, zoals in het geval van voormalig redacteur van De Waarheid Koejemans en de zwager van wijlen CPN-fractievoorzitter Marcus Bakker. Door een intensieve samenwerking met de erkende vakbonden konden radicale arbeiders geweerd worden uit de vakbeweging.

De strijd tegen het communisme werd door de BVD vooral opgevat als een strijd tegen een binnenlandse beweging, ook al werd die beweging door de Communistische Partij Nederland (CPN) vertegenwoordigd in het parlement en hielden de leden zich volledig aan de Nederlandse wet. De BVD had nota bene zelf in een vroeg stadium geconstateerd dat er van deze beweging voor de Nederlandse democratie weinig dreiging uitging.

Een groot deel van het publiek nam de algemene dreiging van het communisme echter serieus. De BVD genoot daarom over het algemeen ook het vertrouwen van de politiek. Controle was lange tijd geen prioriteit bij de verantwoordelijke ministers en de (geheime) Kamercommissie, die zelden bijeen kwam. De dienst kreeg bij gebrek aan wettelijke onderbouwing maximale ruimte, tot vele jaren nadat het parlement van de minister van Binnenlandse Zaken de verzekering kreeg dat de CPN niet langer gevolgd zou worden.

Alle kritiek op de BVD vanuit de samenleving kon worden afgeweerd met een beroep op geheimhouding, het landsbelang en de nationale veiligheid. Pas na de ontmanteling van het communisme in Oost-Europa en de opheffing van de CPN verlegde de BVD de aandacht in een andere richting. Maar de geheime dienst noch de politiek hebben ooit afstand genomen van de oude (wan) praktijken. Een verantwoording voor het verleden heeft nooit plaatsgevonden, excuses zijn nimmer gemaakt.

ONVERWERKT VERLEDEN

De BVD-archieven zijn nog steeds moeilijk toegankelijk. Wie wil achterhalen hoe de dienst in het verleden heeft gehandeld, krijgt hoogstens verminkte documenten toegezonden waarin een groot deel van de informatie is weg gelakt. De AIVD heeft het BVD-verleden kennelijk nog niet achter zich gelaten.

Bij de goedkeuring van de nieuwe WIV 2017 heeft een meerderheid in het parlement zich laten overtuigen dat deze wet voldoende bescherming biedt voor burgers. Maar het papier is geduldig. Kunnen we er op vertrouwen dat een dienst die geen afstand heeft gedaan van een dubieus verleden in de huidige praktijk wél de nodige zorgvuldigheid zal betrachten?

NEDERLAND KOPLOPER BULKINTERCEPTIE?

Lotte Houwing, Transnational Institute

In de WIV 2017 worden vergaande bevoegdheden aan de Nederlandse inlichtingen- en veiligheidsdiensten toegekend. In vergelijking met Britse en Duitse wetgeving levert dat een aantal overeenkomsten en verschillen op.

De Duitse en Britse wetgeving bieden net als de WIV 2017 de inlichtingendiensten de bevoegdheid om communicatie in bulk van het internet te tappen. Bulk betekent dat de diensten grote hoeveelheden communicatie tegelijkertijd kunnen afluisteren zonder selectie, dus van ieder individu in een bepaalde stad of zelfs land.

Het meest opvallende verschil is dat de WIV 2017 geen onderscheid maakt tussen binnenlandse communicatie (communicatie die wordt verstuurd en/of ontvangen door eigen burgers of mensen binnen Nederland) en buitenlandse communicatie (die wordt verstuurd en/of ontvangen door mensen die niet over de Nederlandse nationaliteit beschikken en zich in het buitenland bevinden).

De WIV 2017 maakt het dus mogelijk om alle binnenlandse én buitenlandse communicatie af te luisteren. In Engeland en Duitsland is bulkinterceptie van binnenlandse communicatie niet toegestaan. De Duitse wetgeving maakt daarnaast nog een onderscheid tussen buitenlandse en buitenlands-binnenlandse communicatie waarvoor verschillende regels gelden. De Duitse wetgeving kent ook specifiekere regelgeving voor bulkinterceptie. Om hiervoor toestemming te krijgen gelden, naast gebruikelijke voorwaarden zoals wat het uiteindelijke doel is van de operatie en wie de doelwitten zijn (zowel groepen mensen, organisaties als individuen), ook specifiekere eisen: de zogenaamde selectoren.

Dit zijn technische details als IP-adres, bestandsformaten (tekst- en/of muziekbestand) en inhoudelijke aspecten als bepaalde woorden. Beide voorwaarden zijn ook in de WIV 2017 opgenomen. De Duitse wetgeving stelt echter duidelijker voorwaarden aan de omvang van de interceptie want zowel een duidelijke geografische afbakening (voor waar er mag worden afgetapt) is vereist, als een duidelijke hoeveelheid procent van de communicatie die mag worden afgetapt met een limiet van maximaal 20 procent. De WIV 2017 is daar niet duidelijk over.

HACK BEVOEGDHEID

De hack bevoegdheid in de Nederlandse WIV 2017 lijkt op het Britse equipment interference. Bij hacken breken de diensten in op je smartphone, laptop of andere apparaten die met het internet verbonden zijn. In zowel Groot-Brittannië als Nederland mogen de

diensten inbreken op apparaten van het doelwit zelf, maar ook op die van derden (zowel bedrijven zoals een internetbedrijf waar het doelwit opslagruimte huurt maar ook individuen die in contact staan met het doelwit).

Daarnaast mogen de diensten softwareprogramma's (malware) installeren op apparaten. Zo krijgen de diensten toegang tot communicatie en opgeslagen gegevens zoals e-mails, foto's, informatie over bezochte websites, kunnen ze personen live observeren (meeluisteren en meekijken) en aftappen.

In Groot-Brittannië krijgen de diensten verdergaande toestemming voor hacken dan in Nederland. Hier moet voor iedere handeling apart toestemming worden gevraagd bij de minister en de toetsingscommissie TIB. In Groot-Brittannië hoeft dat niet: de toestemming is overkoepelend en het gaat om het uiteindelijke doel van de operatie.

Wanneer de Britse diensten bijvoorbeeld brede toestemming krijgen om dhr. Buma te hacken, mogen zij in dat kader ook dhr. De Jonge hacken. Dit maakt dan onderdeel uit van de brede toestemming. Volgens de WIV 2017 vereist het hacken van De Jonge echter een aparte toestemming. Voor live communicatie, bijvoorbeeld een Skype-gesprek, moeten de Britse diensten wel apart toestemming vragen.

In het Duitse stelsel is er niet één hack bevoegdheid vastgelegd. Met de zogenoemde Quellen-TKÜ mogen de diensten op geautomatiseerde werken (smartphones, tablets, op het internet aangesloten apparaten) inbreken om lopende communicatie te monitoren, ook jegens derden. Een andere Duitse bevoegdheid, online search, maakt het mogelijk om op afstand in te breken op de apparaten. Dit mag niet gebruikt worden om derden, anderen dan het doelwit, te hacken.

Over de samenwerking en het uitwisselen van informatie met buitenlandse diensten wordt veel geheim gehouden. Het is echter duidelijk dat Nederland een tegengesteld uitgangspunt hanteert dan de grote buurlanden. Volgens de Duitse wet kan informatie alleen worden gedeeld bij een duidelijk en goedgekeurd doel. De Britse wet staat het delen van informatie toe, onder de voorwaarde dat een buitenlandse dienst niet meer informatie verkrijgt dan strikt noodzakelijk is voor een goede taakuitoefening.

WIJ DELEN INFORMATIE, TENZIJ...

Volgens de WIV 2017 kunnen inlichtingen in het kader van samenwerking gedeeld worden, tenzij dit onverenigbaar is met een goede taakuitoefening of met de belangen van de Nederlandse diensten zelf. Tegenover het 'wij delen informatie alleen als...' uitgangspunt van Duitsland en Groot-Brittannië, baseert Nederland zich dus op het uitgangspunt 'wij delen informatie, tenzij...'

In de WIV 2017 worden twee bevoegdheden geïntroduceerd die niet voorkomen in de Britse en Duitse wetgeving, namelijk het maken van de DNA-profielen en het opzetten van de DNA-databank en de real-time toegang tot databanken van verschillende overheidsdiensten, vervoerders en financiële instellingen. Het is opmerkelijk dat Nederland hiermee verder gaat dan haar buurlanden.

In de afgelopen jaren zijn bij wetgeving in verschillende landen, waaronder Nederland, meer en ingrijpender bevoegdheden aan de inlichtingendiensten toegekend. Hoewel er sprake is van een trend, zijn er ook duidelijke verschillen waarneembaar tussen landen. Zo zijn er koplopers, zoals Groot-Brittannië en de Verenigde Staten, die het verst willen ingrijpen in het leven van burgers.

Hierbij moet wel worden aangetekend dat de rechter de Britse wet recentelijk in hoger beroep onrechtmatig heeft verklaard. De consequenties hiervan zijn vooralsnog onduidelijk. Nederland sluit zich met de WIV 2017 aan bij de kopgroep van de Britten en de Amerikanen. Nederland had ook Duitsland kunnen volgen.

'Zo krijgen de diensten toegang tot communicatie en opgeslagen gegevens zoals e-mails, foto's, informatie over bezochte websites...'

SCHADE BURGER DOOR WIV 2017 IS IRRELEVANT

Bart van der Sloot, Tilburg University

De nieuwe Wet op de Inlichtingen- en Veiligheidsdiensten (WIV 2017) zou volgens velen nodig zijn in de strijd tegen terrorisme. Vaak wordt er daarbij op gewezen dat bij bulkinterceptie van metadata de privacy van burgers niet wezenlijk wordt aangetast. Juist grootschalige gegevensverzamelingsprocessen zijn er immers niet op gericht om zaken te weten te komen over concrete individuen.

Dit argument raakt ook aan een basaal uitgangspunt dat zowel in de privacyliteratuur als -jurisprudentie wordt omarmt, namelijk dat burgers alleen een beroep kunnen doen op hun recht op privacy als zij kunnen aantonen direct en individueel geraakt te zijn. Dat wordt in de literatuur wel het non-interference principe genoemd, waaruit volgt dat er bij een interference een inbreuk op een recht is gepleegd.

Dit uitgangspunt komt echter steeds meer onder druk te staan in het tijdperk van Big Data – dataverzamelingsprocessen worden immers steeds groter en het individuele element wordt steeds incidenteler. De meeste traditionele privacyschendingen zijn duidelijk afgebakend in persoon, tijd en plaats.

Om zeven uur 's ochtends trad de politie het huis van meneer De Bruijn binnen; van 9 oktober tot 11 november is de telefoon van mevrouw De Wit afgeluisterd. Dit ligt echter anders bij moderne privacyvraagstukken die vaak draaien om grote gegevensverzamelingsprocessen die nauwelijks in tijd, ruimte en persoon zijn af te bakenen en een structureel en voortdurend onderdeel vormen van de modus operandi van overheidsdiensten.

BIG DATA PROCESSEN

Het probleem van de talloze camera's die op vrijwel elke straathoek van grote steden zijn te vinden, is niet dat ze mij als concreet persoon treffen. Ze filmen iedereen die zich binnen het bereik van de camera's bevindt, overal en altijd. Welke nadelige gevolgen ondervindt een individu eigenlijk als hij gefilmd wordt op straat door een bewakingscamera? Welke concrete schade heeft de gegevensverzameling door de National Security Agency (NSA) gedaan aan de individuele belangen van een gewone Amerikaanse of Europese burger?

Het probleem van deze Big Data processen is niet dat ze mij als persoon concreet en individueel treffen, het probleem is gelinkt aan hoe de overheid haar macht inzet en welke waarborgen er zijn om willekeurige, ongerichte machtsinzet tegen te gaan. Daarom wordt in de literatuur in toenemende mate gesuggereerd dat het liberale non-interference principe moet worden aangevuld met het non-domination principe dat als uitgangspunt wordt genomen in de Amerikaanse republikeinse literatuur.

Om het onderscheid tussen de twee stromingen te duiden, wordt vaak verwezen naar slavernij. Vanuit het uitgangspunt van vrijheid als non-interference zal worden verwezen naar fysieke en mogelijke seksuele uitbuiting, geweld en in het algemeen de beperkingen

die de slaaf heeft in het uitoefenen van zijn autonomie. Stel echter dat de slavenhouder zijn macht niet gebruikt om de slaven te onderdrukken – de slaven zijn helemaal vrij om te doen en te laten wat ze willen. Wat is dan het probleem?

Volgens het non-domination principe is deze relatie alsnog problematisch. Ten eerste omdat de machtsrelatie absoluut is en ten tweede omdat er geen waarborgen gelden tegen willekeurig machtsgebruik – de slavenhouder kan op elk moment besluiten om zijn macht toch in te zetten, op elke wijze die hem goeddunkt. Het gaat er dus niet om of de macht wordt gebruikt, maar of de macht kán worden gebruikt, en de manier waarop die kan worden ingezet, namelijk willekeurig, al naar gelang de grillen van de machthebber.

MACHTSMISBRUIK

Interessant is dat het Europees Hof voor de Rechten van de Mens (EHRM) bereid lijkt om de nadruk op inbreuken en individuele schade te laten varen en in zaken die draaien om massasurveillance een Amerikaanse republikeinse benadering te omarmen.

Allereerst stelt het dat een concrete 'inbreuk' op het recht op privacy niet alleen moet zijn gestoeld op een wettelijke grondslag, maar dat ook de quality of the law moet zijn gewaarborgd. Daarnaast heeft het EHRM geoordeeld dat in zaken die draaien om massasurveillance de vraag naar een concrete inbreuk en individuele schade kan worden losgelaten en in plaats daarvan kan worden gekeken naar de toekenning van macht aan overheidsdiensten als zodanig, het potentiële gevaar voor machtsmisbruik en de in een nationale wet vervatte waarborgen die dergelijk misbruik kunnen voorkomen.

Hiermee wordt een opening geboden om het non-interference principe te laten vallen, aangezien de concrete inbreuk en daaruit volgende schade niet langer centraal staat. Of inlichtingendiensten legitiem handelen moet dus niet alleen worden behandeld aan de hand van de vraag of zij een concrete inbreuk maken op de rechten van specifieke individuen, maar meer in het algemeen. Welke macht zij hebben, hoe die is ingekaderd en welke gevaren er zijn voor machtsmisbruik.

SOCIAL MEDIA SURVEILLANCE

Buro Jansen & Janssen

De in opdracht van politiediensten uitgevoerde social media surveillance staat op gespannen voet met de vrijheid van meningsuiting en de vrijheid van vergadering en betoging.

Met de Wet op de Inlichtingen en Veiligheidsdiensten 2017 krijgen de inlichtingendiensten meer mogelijkheden om op grote schaal communicatie van burgers af te tappen. De meeste mensen zullen echter nauwelijks beseffen dat de Nederlandse politie al op grote schaal burgers op social media in de gaten houdt.

De overheid is weinig mededeelzaam over het plaatsvinden van social media surveillance. Uit documenten die door Buro Jansen & Janssen in 2016 en 2017 via een beroep op de Wet Openbaarheid Bestuur (WOB) zijn verkregen blijkt echter dat de Nederlandse politie in toenemende mate aan social media surveillance doet en hierbij samenwerkt met de bedrijven Coosto (sinds 2012), OBI4wan en HowAboutYou (sinds 2013). Ook de Nationaal Coördinator Terrorisme en Veiligheid (NCTV) maakt sinds 2011 gebruik van de diensten van Coosto.

MONITORING

Coosto, OBI4wan, HowAboutYou zijn Nederlandse social media monitoring bedrijven die tools aanbieden op het terrein van reputatiemanagement en webcare. Tot hun klantenkring behoren bedrijven en overheidsorganen die negatieve publiciteit willen tegengaan. Bovengenoemde bedrijven verzamelen data met zoekmachines die het internet afspeuren. Deze data komen in principe van open bronnen (informatie die door bedrijven en individuen op het internet wordt gedeeld).

Alle verzamelde informatie wordt bewaard, ook berichten die mensen zelf van hun social media account hebben verwijderd. De genoemde bedrijven hebben van deze online en social media data handelswaar gemaakt. Essentieel onderdeel van reputatiemanagement is de sentiment analyse: de data wordt voorzien van een label goed/positief, slecht/negatief en neutraal. Het gaat natuurlijk vooral om negatieve berichtgeving waar een producent snel op wil reageren.

Dat de Nederlandse politie interesse heeft in de diensten en tools van deze drie bedrijven is op zich niet verwonderlijk. Social media data zijn een belangrijke bron van OSINT (Open Source INTelligence), van oudsher een typisch 'product' van inlichtingendiensten, dat ook steeds belangrijker wordt binnen de politiediensten.
Uit de WOB-documenten blijkt dat politiekorpsen al een aantal jaren experimenteren met social media surveillance en dat de politie sinds 2013 een meer gecentraliseerde aanpak ontwikkelt.
In een document uit 2013 spreekt de politie de ambitie uit om social media surveillance een vast onderdeel

van het dagelijkse politiewerk te maken: 'Door de informatieorganisatie in de eenheden wordt er dagelijks online een structurele monitor gedraaid', aldus het document. Twee jaar later, in 2015, wordt het belang van OSINT veelvuldig benadrukt in een adviesrapport. De politie voert ondertussen dag en nacht online en social media surveillance uit, zo blijkt uit dit rapport.

VERKEERD SENTIMENT

De politie gebruikt niet alleen de tools van de bedrijven maar ook de sentiment analyse en denkt dat dit een bijdrage kan leveren aan het politiewerk. Aan de hand van de gelabelde berichten (goed/positief, slecht/negatief en neutraal) kunnen personen dus worden geprofileerd of van een risicoprofiel worden voorzien.

Bedrijven als Coosto en OBI4wan presenteren sentiment analyse doorgaans als een wetenschappelijke methode. Er bestaat echter geen wetenschappelijke onderbouwing van de kwaliteit, nauwkeurigheid en totstandkoming van de analyses. De effectiviteit van sentiment analyse is dan ook ongewis. Het is de de vraag in hoeverre het bijdraagt aan de effectiviteit van politiewerk, of vooral bijdraagt aan het ongefundeerd verdacht maken van (groepen) mensen.

Het is verontrustend dat de politie geen kritische kanttekeningen plaatst bij de betrouwbaarheid en nauwkeurigheid van de sentiment analyse. In de via de WOB openbaar gemaakte beleidsdocumenten wordt hier met geen woord over gesproken.

GRONDRECHTEN

Social media surveillance staat op gespannen voet met de vrijheid van meningsuiting en de vrijheid van vergadering en betoging. Het wordt ingezet om kritische burgers en protestgroepen in de gaten te houden. Uit de WOB-documenten blijkt dat het kan gaan om demonstraties, manifestaties, maar ook om voetbalwedstrijden of feesten van een motorclub.

De politie lijkt zich echter niet bezig te houden met de vraag hoe social media surveillance zich verhoudt tot de grondrechten van haar burgers. In de WOB-documenten ontbreken de juridische kaders hiervoor volledig. Veelzeggend is de passage in een intern beleidsdocument uit 2015 waarin wordt vermeld 'dat de juridische kaders voor de gebruikers van de tools nog moeten worden opgesteld'.

Social media surveillance staat ook op gespannen voet met de privacywetgeving. De politie mag niet ongelimiteerd persoonsgegevens verzamelen, verwerken en bewaren. Haar beleid ten aanzien van opslag en verwerking van persoonsgegevens is wettelijk geregeld en er zijn maximum bewaartermijnen.

Door gebruik te maken van de diensten van Coosto, OBI4wan en HowAboutYou omzeilt de politie deze wettelijke beperkingen. De online en social media gegevens die deze bedrijven verzamelen zijn persoonsgegevens, hetgeen ook wordt bevestigd in hun privacyverklaringen. Geen van de bedrijven heeft de verwerken van persoonsgegevens echter gemeld bij de Autoriteit Persoonsgegevens (AP), of haar voorganger het College Bescherming Persoonsgegevens. Desbetreffende bedrijven worden al tien jaar niet gecontroleerd door de AP.

DE SURVEILLANCETREIN DENDERT VOORT

De Nederlandse politie doet de afgelopen jaren steeds meer aan social media surveillance. De AIVD en de MIVD hebben nooit bekend gemaakt of zij gebruik maken van social media surveillance. Wel verklaarde voormalig minister Blok (Wonen en Rijksdienst) in 2013 dat de Ministeries van Binnenlandse Zaken en Koninkrijksrelaties en Defensie, die verantwoordelijk zijn voor respectievelijk de AIVD en MIVD, Coosto als leverancier hebben. Het is aannemelijk dat ook de inlichtingendiensten aan social media surveillance doen, maar de WOB-documenten bieden hierover geen nader uitsluitsel.

De trein van social media surveillance dendert voort, hoewel het middel op gespannen voet staat met de grondrechten en de bescherming van persoonsgegevens en de gehanteerde methode van sentiment analyse discutabel is. De overheid, social media platforms en sociale monitoring bedrijven zijn niet transparant en leggen geen politieke of maatschappelijke verantwoording af over de wenselijkheid en risico's van social media surveillance. Dat is verontrustend.

BURO JANSEN & JANSSEN

Buro Jansen & Janssen is een onafhankelijke organisatie die al dertig jaar onderzoek doet naar de politie en de inlichtingendiensten. Alle publicaties van Buro Jansen & Janssen zijn te vinden op de website burojansen.nl. Buro Jansen & Janssen zet zich ook in om de vernietiging van de archieven van inlichtingendiensten te voorkomen en deze openbaar te maken, zie hiervoor voorkomvernietiging.nl. Stukken die openbaar worden gemaakt worden gepubliceerd op hetnationaalveiligheidsarchief.nl of openbaarheid.nl. Op de laatste website vindt u documenten over allerlei onderwerpen die openbaar zijn gemaakt na WOB verzoeken van Buro Jansen & Janssen. Tot slot zijn er websites waar kort ingegaan wordt op de actualiteiten zoals justitieenveiligheid.nl en inlichtingenenterrorisme.nl.

COLOFON

Dit magazine is een uitgave van Buro Jansen & Janssen in het kader van het referendum over de WIV 2017. De artikelen zijn uit deze uitgave zijn ook te vinden op www.wiv2017.nl, waar u ook kunt reageren.

Aan de publicatie werkten onder andere mee:
Rick van Amersfoort, Claudius, Jurre van Bergen, Jos van Dijk, Teun van Dongen, Dupont, Hernandez, Hessel Dokkum, Lotte Houwing, Kees Kalkman, Maikel van Leeuwen, Du Pang, Bart van der Sloot, Skafti, Marc Stolwijk, Schulze, Erik Timmerman, Tjepkema (auteur op justitieenveiligheid.nl), Alex van Veen, DrWhax, Tanja IJzer.

Ontwerp:
Marleen van der Zanden

Foto verantwoording:
Foto pagina 13 van Bayke de Vries (De oren van Burum, Wikimedia Commons); Foto pagina 18 van Bert Kaufmann (It Greate Ear tussen de koeien, Wikimedia Commons); Foto pagina 27 van Anne Geene (Het antenneveld in Eibergen voor De Correspondent); Foto pagina 30 van Molair (AIVD Zoetermeer).

Dit magazine is mede mogelijk gemaakt met steun van onze donateurs en de referendumcommissie.

Buro Jansen & Janssen
Postbus 10591 1001EN Amsterdam
020-6123202 06-34339533
info@burojansen.nl
www.burojansen.nl

Word donateur
NL56 INGB 0000 6039 04
t.n.v. Stichting Res Publica


Commissie voor de Inlichtingen- en Veiligheidsdiensten
Militaire Inlichtingen- en Veiligheidsdienst
Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten
Joint Sigint Cyber Unit
Wet op de Inlichtingen- en Veiligheidsdiensten
Algemene Inlichtingen- en Veiligheidsdienst
Nationaal Cyber Security Centrum
National Security Agency
Toetsingscommissie Inzet Bevoegdheden