Wordt het veiliger door de nieuwe Wet op de Inlichtingen en Veiligheidsdiensten?

Terwijl het politieke debat rond de gemeenteraadsverkiezingen van 21 maart in volle gang is, speelt de discussie rond de nieuwe Wet op de Inlichtingen- en Veiligheidsdiensten zich in de luwte af. Politieke partijen bezigen wat algemeenheden over een balans tussen veiligheid en privacy, mensenrechtenvoorvechters geven toe dat er de nodige waarborgen in de wet zijn getroffen en Rob Bertholee, de Directeur van de Algemene Inlichtingen- en Veiligheidsdienst (AIVD), stelt zich op als streng maar empathisch vaderfiguur dat de natie behoedt voor dreiging van buitenaf.

Onderzoek toont aan dat de meeste burgers bij het referendum voor de nieuwe wet zullen stemmen als die de veiligheid vergroot. De wet geeft de AIVD de bevoegdheid om op grote schaal communicatiegegevens van onverdachte burgers te verzamelen, het zogenoemde sleepnet. Daarnaast kunnen gegevens worden uitgewisseld met zusterorganisaties in andere landen en krijgt de inlichtingendienst ruimere bevoegdheden om online data te verzamelen over potentiële verdachten, ook wel targets genoemd. De wet verlegt daarmee de focus van het inlichtingenwerk van het oude spionnenwerk, waarbij wordt geïnfiltreerd in netwerken en verdachten worden geobserveerd en gefrustreerd, naar data-gedreven opsporing en massa surveillance, waarbij terroristen op basis van profielen en computeranalyses worden opgespoord.

Maar wordt Nederland veiliger door de inzet van nieuwe data-technologieën? Dat is helemaal niet zo zeker. Allereerst zijn er algemene zorgen over de inzet van data-analyses en -voorspellingen, die blijken er namelijk vaak naast te zitten. Vlak voor de Amerikaanse verkiezingen voorspelden Big Data programma's bijvoorbeeld met 99,9% zekerheid dat Hilary Clinton zou winnen, de transitie naar een datagedreven aanpak bij de belastingdienst is vooralsnog een fiasco en ook de op dataprofielen gebaseerde advertenties op het internet slaan vaak de plank mis. Big Data gaat om kansberekening en er is dus altijd een foutmarge; juist bij terrorismebestrijding is dat geen pré.

Maar in het veiligheidsdomein werkt het toch wel? Ook dat is niet zeker. Zo is in binnen- en buitenland veel geëxperimenteerd met predictive policing, voorspellend politiewerk op basis van dataprofielen. Na uitvoerig onderzoek is gebleken dat er geen bewijs is dat het hierdoor ook veiliger is geworden. Predictive policing blijkt simpelweg niet effectief; het is geen goed middel om boeven mee te vangen. Voor het opsporen van terroristen is de effectiviteit van data-analyses eigenlijk nog veel beperkter. Data analyses gaan uit van grote hoeveelheden data en het vinden van algemene patronen. Terwijl het ten aanzien van daders van moorden, diefstallen en uitingsdelicten nog mogelijk is om algemene kenmerken te destilleren, gedragen terroristen zich vaak als een lone wolf en is hun gedrag nauwelijks te voorspellen door middel van data-analyse.

Maar de dataverzameling kan toch geen kwaad? Helaas is dat niet het geval. Allereerst worden er natuurlijk middelen en mankracht geïnvesteerd in een mogelijk ineffectieve methode, terwijl investeringen in andere methodes wel doeltreffend of vele malen effectiever zouden zijn. Alhoewel de nieuwe bevoegdheden in Nederland worden gepresenteerd als een vooruitgang – eindelijk mag de dienst nieuwe methoden gebruiken – is in feite het omgekeerde waar. Veel buitenlandse inlichtingendiensten die al langer hebben geëxperimenteerd met data-analyses zijn daar naar verluidt weer van teruggekomen of hebben hun Big Data programma sterk

teruggeschroefd. Ouderwets inlichtingenwerk blijkt eigenlijk helemaal zo gek nog niet.

Maar het hebben van data is toch waardevol? Ook dat is niet per sé het geval. Het probleem van veel inlichtingendiensten is juist dat zij te veel data hebben verzameld. Bij vrijwel iedereen kan uit de data-analyse wel iets opmerkelijks worden geconstateerd – een raar telefoontje, het bezoeken van een verdachte website, het gebruik van bepaalde woorden in e-mails. Sommige inlichtingendiensten hebben dan ook meer 10.000 personen in hun vizier, terwijl zij niet de mankracht hebben om nader onderzoek te doen naar al die verdachten. Vaak blijkt dan ook nadat er een aanslag is geweest dat de diensten al informatie hadden over de verdachte, zonder dat daar actie op ondernomen is. Hoe meer data er worden verzameld, hoe vervuilder het beeld raakt en hoe minder groot de kans wordt dat de echte probleemgevallen er tussen uit worden gehaald.

Maar er zijn toch voldoende garanties om de veiligheid te waarborgen? Ook dat valt te bezien. De AIVD is de overheidsdienst met veruit de grootste macht en bevoegdheden en tegelijkertijd met de minste rechterlijke controle en transparantie. De AIVD wordt dus steeds machtiger en krijgt steeds meer informatie over de burger, terwijl de dienst zelf nagenoeg ondoorgrondelijk en oncontroleerbaar blijft. Naast het gevaar voor doelbewust machtsmisbruik en datamanipulatie is het probleem dat de verzamelde gegevens jaren worden bewaard. Dat zelfs de veiligheidsmaatregelen van de AIVD te kraken zijn bleek onlangs toen huisleverancier FOX-IT werd gehackt en een aantal vertrouwelijke bestanden werden gestolen. Daarbij komt dat er data worden gedeeld met tientallen inlichtingendiensten in andere landen. Garanties dat de door de AIVD verzamelde gegevens door buitenlandse diensten niet worden misbruikt zijn er niet. Ook dit vormt een veiligheidsrisico.

Terwijl het dus onduidelijk is in hoeverre de nieuwe bevoegdheden de veiligheid zullen vergroten, is zeker dat er tal van inherente problemen en risico's aan verbonden zijn. Als veiligheid de doorslaggevende factor is, dan is de keuze woensdag nog niet zo eenvoudig.

Bart van der Sloot
16-03-2018