

Geachte leden van de vaste commissies voor Binnenlandse Zaken, Defensie en Veiligheid en Justitie,

In deze notitie zal ik, namens de WRR, ingaan op het wetsvoorstel ‘Wet op de inlichtingen- en veiligheidsdiensten 20..’ ten behoeve van het rondetafelgesprek op donderdag 15 december 2016. Ik zal me daarbij in hoofdzaak baseren op het WRR-rapport ‘Big Data in een vrije en veilige samenleving’ en daarmee op het onderwerp van de grootschalige data-analyse.

Uitbreiding bevoegdheden: noodzakelijk en onmogelijk te beoordelen

In een digitale wereld ligt het voor de hand dat inlichtingen- en veiligheidsdiensten in staat moeten worden gesteld dataverkeer te verzamelen en analyseren. Wat de bijdrage daarvan aan de nationale veiligheid is, is van de buitenkant echter niet eenvoudig vast te stellen. Het algemene publiek moet het op dat punt doen met wat de diensten zelf naar buiten brengen en wat via de rapportages van de CTIVD naar buiten komt. Uw kamer wordt in belangrijke mate geïnformeerd via de CIV, maar die beraadslagingen zijn geheim. Het feit dat met het uitbreiden van de bevoegdheden de hoeveelheid *ongerichte informatie over grote groepen burgers* enorm zal toenemen, onderstreept het belang om het werk van de diensten veel beter te volgen en toetsen. Op dit punt is er ruimte voor verbetering in de WIV.

Inlichtingen- en veiligheidsdiensten en Big Data

Big Data is meer dan alleen veel data. Het cruciale punt is dat de werkwijze anders is dan bij een gewone opsporingmethode. Het klassieke dataonderzoek brengt met behulp van data de handel, wandel en contacten van een *verdachte* in kaart. In een ideaaltypische Big Data analyse gaat men op zoek naar correlaties in een dataset zonder een verdachte in beeld te hebben. Dat kan verrassende inzichten bieden maar geeft geen inzicht in causaliteit. Dat betekent ook dat de logica van Big Data altijd in de richting wijst van het verzamelen van méér data omdat dit de analyse ten goede komt. Een volledig ongestructureerde analyse zal in de praktijk van de diensten niet vaak voorkomen. Wel zal men op basis van profielen grote datasets doorkammen op zoek naar personen/organisaties/transacties die aan bepaalde profielen voldoen. De patroonherkenning van Big Data brengt op basis van statistische waarschijnlijkheden echter veel meer mensen onder de aandacht van de diensten dan een onderzoek dat vanuit een concrete verdenking vertrekt. Big Data brengt niet alleen veel meer data van veel meer mensen in de databanken van de diensten onder (stap 1, verzameling), het betreft ook veel meer mensen in de onderzoeken van de diensten (stap 2, analyse). Dat betekent dat privacy en grondrechten in beide fases extra onder druk komen te staan voor een veel grotere groep mensen. In de analysefase zijn foutmarges – de tolerantie voor vals positieven en vals negatieven – en de kwaliteit van profielen en van de analyse (algoritmen en dataselectie) van cruciaal belang voor zowel het werk van de diensten als voor de fundamentele rechten van burgers.

Versterking van het toezicht op de fase van analyse.

De meeste versterkingen van het toezicht in het wetsvoorstel betreffen het toezicht voorafgaand aan de inzet van middelen. Gezien het belang van de analysefase vindt de WRR juist dat deze fase veel sterker onder toezicht zou moeten komen te staan. De diensten zouden een wettelijke zorgplicht moeten krijgen waarin het borgen van de kwaliteit en de

toegankelijkheid van de analyse voor het toezicht centraal staan. Centrale elementen daarvan zijn:

- Zorgen dat gegevens up to date zijn en dat gecorrigeerd wordt voor de bias in datasets. Deze plicht strekt zich ook uit tot gegevens die de diensten van derden verkrijgen.
- De algoritmes en methoden die bij data-analyses worden gebruikt moeten deugdelijk zijn, aan de wetenschappelijke criteria voor goed (statistisch) onderzoek voldoen en voor toezicht toegankelijk zijn.
- Onderzoeksresultaten, profielen en foutmarges moeten op hun merites worden beoordeeld: de diensten moeten duidelijk kunnen maken hoe zij tot bepaalde uitkomsten komen.

De zorgplicht is de basis voor het versterken van het toezicht op de fase van de analyse – dat nu ontbreekt - die volgens de WRR bij de CTIVD belegd moet worden. De CTIVD kan reviews maken over Big Data projecten en in het bijzonder toezien op de gemaakte keuzes inzake data en methode van analyse. Deze review toetst ook of er aan de zorgplicht is voldaan. De CTIVD moet daartoe wel in staat worden gesteld in termen van toegang, technische kennis en middelen. In haar ‘Zienswijze van de CTIVD op het wetsvoorstel Wiv 20..’ heeft de CTIVD zelf een gedetailleerde uitwerking gegeven van een dergelijke zorgplicht.

Transparantere werkwijze

Aangezien met de uitbreiding van bevoegdheden veel meer mensen in de informatie-sfeer van de diensten terecht komen, vereist dit meer transparantie. De afweging tussen noodzakelijke geheimhouding en transparantie valt in Nederland te vaak – en met weinig onderbouwing – in het voordeel van de geheimhouding uit. In het algemeen vindt de WRR dat de transparantie van de gegevensverwerking kan worden vergroot. Een beter evenwicht tussen het vereiste van geheimhouding en het belang van openbaarheid over Big Data-toepassingen die aan fundamentele vrijheden raken, is noodzakelijk.

Transparantie naar volksvertegenwoordiging en burgers verloopt getrapt. Door de toezichthouder meer inzicht te geven in de analysefase vergroot dat het inzicht in de werkwijze en in de risico's voor fundamentele rechten. De toezichthouder rapporteert vervolgens aan uw kamer. Omdat de verantwoording getrapt verloopt, is er ruimte is voor een grotere mate van transparantie en detail in de rapportages aan de toezichthouder. In het openbare rapport van de toezichthouder aan de Kamer wordt ‘het geheim van de smid’ (de specifieke methoden) niet opgenomen. Maar het is wel op basis van kennis en inzicht daarvan opgesteld. Wat de WRR betreft zou het streven daarbij moeten zijn om het democratische debat zoveel mogelijk in openbare zittingen van de vaste Kamercommissies van Binnenlandse Zaken een Defensie te doen en alleen waar nodig in geheime zittingen en in de CIV.

Chilling effects en persoonlijke vrijheid

Naast schendingen van individuele rechten als privacy schuilt het grootse gevaar erin dat nieuwe bevoegdheden om onze veiligheid te beschermen sluipenderwijs omslaan in het tegendeel. De WRR wees in zijn rapport op de beschermende werking van afstand – van andere burgers, maar zeker ook de overheid – voor de persoonlijke vrijheid van burgers. Big Data doet afbreuk aan die afstand. Een samenleving waarin burgers zich voortdurend gevolgd en bekeken voelen kan ertoe leiden dat burgers zich anders gaan gedragen. Dit noemt men wel *chilling effects*. Sommigen zullen hun gedrag aanpassen om zo normaal mogelijk te lijken, anderen zullen wellicht zoveel mogelijk buiten beeld proberen te geraken. In beide gevallen wordt hun vrijheid ingeperkt. Juist om dit te voorkomen – maar ook om de valse indruk te voorkomen dat de ontwikkelingen de verkeerde kant uitgaan – is het van groot belang om nu te investeren in meer transparantie en een beter toezicht.

Prof. Dr. Dennis Broeders
Wetenschappelijke Raad voor het Regeringsbeleid