WRR

WETENSCHAPPELIJKE RAAD VOOR HET REGERINGSBELEID

Synopsis van
WRR-rapport

95

BIG DATA IN EEN VRIJE EN VEILIGE SAMENLEVING

SYNOPSIS

Big Data in een vrije en veilige samenleving

De Wetenschappelijke Raad voor het Regeringsbeleid werd in voorlopige vorm ingesteld in 1972. Bij wet van 30 juni 1976 (Stb. 413) is de positie van de raad definitief geregeld. De huidige zittingsperiode loopt tot 31 december 2017.
Ingevolge de wet heeft de raad tot taak ten behoeve van het regeringsbeleid wetenschappelijke informatie te verschaffen over ontwikkelingen die op langere termijn de samenleving kunnen beïnvloeden. De raad wordt geacht daarbij tijdig te wijzen op tegenstrijdigheden en te verwachten knelpunten en zich te richten op het formuleren van probleemstellingen ten aanzien van de grote beleidsvraagstukken, alsmede op het aangeven van beleidsalternatieven.
Volgens de wet stelt de WRR zijn eigen werkprogramma vast, na overleg met de minister-president die hiertoe de Raad van Ministers hoort.
De samenstelling van de raad is:
prof. dr. A.W.A. Boot
prof. dr. mr. M.A.P. Bovens
prof. dr. G.B.M. Engbersen
prof. mr. dr. E.M.H. Hirsch Ballin
prof. dr. J.A. Knottnerus (voorzitter)
prof. dr. M. de Visser
prof. dr. C.G. de Vries (adviserend raadslid)
prof. dr. ir. M.P.C. Weijnen
Secretaris: dr. F.W.A. Brom

Wetenschappelijke Raad voor het Regeringsbeleid
Buitenhof 34
Postbus 20004
2500 EA Den Haag
Telefoon 070-356 46 00
E-mail info@wrr.nl
Website www.wrr.nl

WRR

WETENSCHAPPELIJKE RAAD VOOR HET REGERINGSBELEID

Big Data in een vrije en veilige samenleving

SYNOPSIS VAN WRR-RAPPORT 95

Wetenschappelijke Raad voor het Regeringsbeleid, Den Haag 2016

Verantwoording
Deze publicatie is een samenvatting van het WRR-Rapport 95 *Big Data in een vrije en veilige samenleving*. Voor een onderbouwing van de in deze publicatie gepresenteerde conclusies en aanbevelingen wordt verwezen naar de uitvoerige analyses van het beleid en de wetenschappelijke literatuur die in dat rapport te vinden zijn.
Het rapport *Big Data in een vrije en veilige samenleving* (ISBN 978 94 6298 357 1) is op 28 april 2016 door de Raad aangeboden aan de regering. Het rapport is te koop in de boekhandel en te bestellen bij Amsterdam University Press. Het rapport kan ook in pdf-formaat gratis worden gedownload op www.wrr.nl.

Samenstelling: WRR
Omslagafbeelding: Textcetera/ cimon communicatie, Den Haag

INHOUD

Samenvatting 7
Big Data en veiligheid 7
Kansen en risico's 8
Mismatch tussen Big Data en de huidige wet- en regelgeving 9
Regulering van data-analyse en -gebruik 9
Toezicht, transparantie en rechterlijke toetsing 10

SAMENVATTING

De WRR analyseert in dit rapport hoe de Nederlandse overheid Big Data op een verantwoorde wijze kan gebruiken. Het rapport richt zich specifiek op (Big) Data-analyses door politie en justitie, de inlichtingen- en veiligheidsdiensten en verschillende organisaties en samenwerkingsverbanden op het gebied van fraudebestrijding. Big Data biedt zeker kansen voor opsporing en surveillance, maar vraagt tevens om sterkere waarborgen voor de vrijheidsrechten van burgers. Het zwaartepunt in de huidige juridische regelgeving ligt op de regulering van het *verzamelen* van data. De WRR pleit ervoor dat die bestaande wetgeving wordt aangevuld met de regulering van en het toezicht op de fases van de *analyse* en het *gebruik* van Big Data.

BIG DATA EN VEILIGHEID

De hoeveelheid beschikbare data over personen en processen is de laatste jaren exponentieel toegenomen. Dat komt vooral omdat veel data tegenwoordig automatisch worden geproduceerd en het bijproduct zijn van dagelijkse handelingen zoals het gebruik van internet, sociale media, mobiele telefoons en verschillende applicaties. Hierdoor worden steeds meer handelingen van individuen digitaal geregistreerd. Bovendien verdubbelt de opslagcapaciteit ongeveer iedere drie jaar en nemen de kosten van dataopslag sterk af. De combinatie van steeds krachtigere computers, betere software, zelflerende algoritmen en *machine learning* biedt kansen voor Big Data-toepassingen. Door het koppelen van databases wordt het mogelijk om nieuwe, praktisch bruikbare kennis te construeren. Behalve commerciële partijen maken ook overheidsorganisaties steeds vaker gebruik van die nieuwe kennis- en datavergaring.

Het is niet gemakkelijk in kaart te brengen hoe en in welke mate Big Data zich in het (Nederlandse) veiligheidsdomein manifesteert. Dit heeft te maken met geheimhouding en het experimentele karakter van sommige toepassingen. Naast het domein van de inlichtingen- en veiligheidsdiensten, de Belastingdienst en fraudebestrijding zijn er vooralsnog weinig echte Big Data-toepassingen in gebruik. Dat komt mede doordat de omschakeling op nieuwe werkwijzen tijd en geld kost en verreikende aanpassingen in de werkorganisatie impliceert. Veel organisaties hebben nog niet de keuze gemaakt om grootschalige, data-gedreven analyses uit te voeren. Door de snelle technologische ontwikkelingen zal deze keuze voor een groeiend aantal organisaties desondanks in de nabije toekomst een reële optie zijn.

KANSEN EN RISICO'S

Big Data heeft voor specifieke vormen van criminaliteit (zoals fraude) al positieve resultaten laten zien, al ontbreekt in veel gevallen een betrouwbare onderbouwing en evaluatie van de effectiviteit van de gebruikte analysemethoden. De geautomatiseerde analyse van grote, gecombineerde gegevensbestanden levert grote tijdwinst op en kan – mits zorgvuldig uitgevoerd – ook in nauwkeurigere uitkomsten resulteren. Organisaties kunnen deze uitkomsten gebruiken om gerichte inspecties uit te voeren. Big Data is tevens nuttig bij de reconstructie van aanslagen en het in kaart brengen van criminele netwerken, met als doel de opsporing van daders te vergemakkelijken. Ook kan Big Data behulpzaam zijn bij het *real time* volgen van ontwikkelingen in crisissituaties of bij *crowd control* rond evenementen. Politiemensen en veiligheidsfunctionarissen kunnen dan snel een beeld krijgen van de situatie ter plaatse. Dit soort toepassingen zal in de nabije toekomst steeds belangrijker worden. We gaan toe naar steeds verdergaande koppelingen van databronnen. Ook zal het steeds aantrekkelijker worden om (ten minste een deel van) het analyseproces te automatiseren. De grens tussen data uit publieke en private bronnen zal vervagen.

Aan Big Data-toepassingen kleven echter ook risico's. Een van de grootste zorgen is de grootschalige inmenging in de persoonlijke levenssfeer. De grootschalige verzameling, opslag en analyse van data door overheden, waaronder inlichtingen- en veiligheidsdiensten, kunnen ertoe leiden dat mensen het gevoel krijgen dat hun privacy en vrije meningsuiting in gevaar zijn, waardoor zij hun gedrag daarop aanpassen. Bovendien worden burgers steeds transparanter voor de overheid, terwijl de profielen, algoritmen en methoden die overheidsorganisaties gebruiken nauwelijks transparant of navolgbaar voor die burgers zijn. Nu met Big Data-toepassingen steeds grotere groepen burgers in beeld komen – naast verdachte ook niet-verdachte burgers – gaat dat gebrek aan transparantie steeds meer wringen. Daarnaast kunnen Big Data-toepassingen leiden tot een toename van sociale stratificatie, met een ongelijke verhouding tussen maatschappelijke groepen als gevolg. Dit gebeurt doordat Big Data onregelmatigheden en afwijkingen in datasets kan reproduceren, resulterend in uitkomsten die een onevenredige sociale impact hebben. Zonder correctie vertaalt zich dit op termijn in een cumulatief nadeel (discriminatie en oneerlijke behandeling) voor bepaalde groepen in de maatschappij. Ook zijn Big Data-toepassingen zeer gevoelig voor 'function creep', oftewel gebruik van gegevens anders dan voor het doel waarvoor de data zijn verzameld. De reden hiervan is dat het secundair gebruik van gegevens bij Big Data-toepassingen een grote meerwaarde oplevert.

MISMATCH TUSSEN BIG DATA EN DE HUIDIGE WET- EN REGELGEVING

De juridische kaders die van toepassing zijn op de gegevensverwerking binnen het veiligheidsdomein zijn vooral gericht op het verzamelen en delen van gegevens. Door het gebruik van Big Data ontstaat echter druk op belangrijke uitgangspunten van deze kaders, zoals doelbinding en noodzakelijkheid. Want in zijn ideaalvorm is Big Data gebaseerd op het principe van ongerichte gegevensverzameling en secundair gebruik van reeds verzamelde gegevens voor andere doeleinden, hetgeen botst met de regelgevende kaders. De wettelijke normen voor het verzamelen van gegevens vereisen daarom aanvulling. Het verzwaren van het huidige kader – met de nadruk op het reguleren van verzamelen en de handhaving van doelbinding en noodzakelijkheid – zou echter een groot deel van de belofte van Big Data in de kiem smoren.

De WRR zet daarom in op een versterking van de regulering van de fases van de *analyse* en het *gebruik* van Big Data-processen. De bestaande en in ontwikkeling zijnde regulering voor het verzamelen van gegevens hebben desondanks ook in het Big Data-tijdperk onverminderd een belangrijke functie. De raad is echter van mening dat er meer winst te behalen valt in de latere fasen van Big Data-processen dan in een intensivering van de regulering van het verzamelen van data. Alleen door extra eisen te stellen aan het toepassen van Big Data-analyses kunnen burgers erop vertrouwen dat de overheid niet sluipenderwijs in hun persoonlijke vrijheid penetreert. Regulering van analyse en gebruik is volgens de raad een *conditio sine qua non* voor het niet zwaarder reguleren van het verzamelen van gegevens.

REGULERING VAN DATA-ANALYSE EN -GEBRUIK

Bij de regulering van de fase van de analyse van gegevens is sprake van een hiaat in de regelgeving. In Big Data-processen zijn de keuzes die in de analysefase worden gemaakt (algoritmen, categorisering, wegingsfactoren enz.) van eminent belang. Juist op dit vlak kunnen zich risico's voordoen zoals discriminatie en te veel pretenderende gegevensanalyses. Op de achtergrond hiervan dreigen negatieve sociale effecten op persoonlijke vrijheden zoals de vrije meningsuiting, die een vitale rol spelen in de democratische rechtsstaat.

Er is daarom aanvullende normering nodig in de vorm van een *wettelijk omschreven zorgplicht*, met algemene vereisten voor de kwaliteit van de data en van de deugdelijkheid van de gehanteerde analysemethoden.

De gegevensverwerkende partijen moeten desgevraagd altijd duidelijk kunnen maken hoe zij tot bepaalde uitkomsten komen. Dat vereist al tijdens de analysefase externe aandacht. Big Data-projecten en -toepassingen in het veiligheidsdomein

moeten onderwerp zijn van een *externe review door de toezichthouder*. Bij gebleken gebreken in de rapportage kan de toezichthouder de audits aanscherpen, opvoeren en in uiterste gevallen overlaten aan een onafhankelijke derde. Een belangrijke vereiste voor deze verscherpte vorm van toezicht is dat toezichthouders zoals de Autoriteit Persoonsgegevens en de Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (CTIVD) hun *technische en statistische capaciteit en expertise versterken.* Ook is het vanwege de potentiële impact van data-gedreven toepassingen in het veiligheidsdomein belangrijk om bij Big Data-projecten vooraf een evaluatiemoment in te plannen. Grote dataverwerkingsprojecten binnen de overheid, vooral door de politie, inlichtingen- en veiligheidsdiensten, inspecties, de Belastingdienst en samenwerkingsorganen op het terrein van misdaad- en fraudebestrijding, moeten een *horizon van 3 tot 5 jaar* krijgen.

Bij het gebruik van de gegevensanalyses in Big Data-processen is de problematiek rond het samenstellen van profielen van belang. De kracht van Big Data-analyses ligt voornamelijk in algemene conclusies en structurele patronen. Bij de toepassing daarvan op concrete situaties en specifieke individuen bestaat altijd een mismatch, omdat een profiel zowel over- als onder-inclusief is. De WRR beveelt aan om het *profileren strakker te reguleren* door nadere regels over toelaatbare foutmarges te stellen, het verbod op geautomatiseerde besluitvorming door computers strikter te handhaven en alert te zijn op semi-automatische besluitvorming. De Nederlandse overheid zou in Europa een voortrekkersrol moeten nemen en ervoor moeten zorgdragen dat geautomatiseerde besluitvorming achterwege blijft. Hiertoe behoren in feite ook de situaties waarin formeel een mens het besluit neemt, maar deze de facto niet afwijkt van het digitale advies.

In het verlengde hiervan beveelt de WRR aan om juridisch te verankeren dat dataanalyses en profielen niet kunnen leiden tot een feitelijke verlegging van de bewijslast. Dat speelt niet zozeer in het strafrecht – waar strikte regels voor bewijsvoering gelden – maar wel in verschillende vormen van surveillance, handhaving en fraudebestrijding.

TOEZICHT, TRANSPARANTIE EN RECHTERLIJKE TOETSING

De toegenomen mogelijkheden om data te verzamelen en te analyseren, vragen om een *versteviging van het onafhankelijke toezicht*. Het toezicht op gegevensverwerking laat tot nu toe veel te wensen over, zeker in het licht van de huidige snelle ontwikkelingen op het gebied van Big Data. Zowel de Autoriteit Persoonsgegevens als de CTIVD is onvoldoende toegerust voor de uitdagingen van het Big Data-tijdperk in termen van bevoegdheden, expertise en financiële middelen. Vele partijen, waaronder de CTIVD zelf, zijn van mening dat de voorgenomen uitbreiding van bevoegdheden van de MIVD en AIVD vraagt om een significante uitbreiding van de capaciteit en expertise van de toezichthouder op alle niveaus. Voor

de parlementaire Commissie voor de Inlichtingen- en Veiligheidsdiensten, die nauwelijks eigen ondersteuning heeft, geldt dat wellicht nog sterker. Hoewel de bevoegdheden en middelen van de Autoriteit Persoonsgegevens als gevolg van de nieuwe Europese verordening gegevensbescherming zullen worden verstevigd, is het voornamelijk aan de nationale wetgever om de bijbehorende financiële middelen, bevoegdheden en capaciteiten toe te kennen. Hier is dus actie van de Nederlandse regering nodig.

Ook op het punt van de transparantie van de dataverwerkingsprocessen van de overheid is nog een wereld te winnen. De gegevensverwerking is in veel gevallen een black box. Individuen kunnen vaak niet weten dat over hen gegevens zijn verzameld en zullen dus niet zo snel hun informatierecht inroepen. Hoewel binnen het veiligheidsdomein geen volledige transparantie kan bestaan vanwege geheimhouding, is desalniettemin op verschillende niveaus een *grotere mate van transparantie* mogelijk. Veel relevante informatie over gegevensverwerking binnen samenwerkingsverbanden op het terrein van fraudebestrijding staat bijvoorbeeld in convenanten en besluiten vermeld, die weliswaar openbaar maar niet erg toegankelijk zijn. Ook is het wenselijk dat organisaties die met Big Data-toepassingen aan de slag gaan, een beleidsplan opstellen waarin zij vermelden welke methoden zij gebruiken, en wat de kosten en de beoogde resultaten zijn. De inlichtingen- en veiligheidsdiensten zouden meer werk kunnen maken van het achteraf inzichtelijk maken van de frequentie waarmee zij bepaalde toepassingen hebben gebruikt en voor welke doeleinden. De beschikbaarheid van dergelijke informatie kan een bijdrage leveren aan een grotere maatschappelijke aanvaardbaarheid van de inzet van Big Data-toepassingen in het veiligheidsdomein.

Veel grote dataverwerkingsprojecten overstijgen het individu in aard en omvang. Daarom is het belangrijk om, naast een inzet op toezicht en transparantie, ook de positie van NGO's en burgerrechtenorganisaties in juridische procedures te versterken. Het is weliswaar primair de verantwoordelijkheid van de wetgevende macht en van het parlement in zijn controlerende functie, om wetgeving en beleid omtrent Big Data-toepassingen te toetsen. Maar burgers kunnen ook direct of via belangenorganisaties stem geven aan hun belang bij vrijheid en veiligheid. In de huidige situatie is het klachtrecht sterk verbonden aan individuele schade en zijn er zeer beperkte mogelijkheden voor collectieve procedures bij de rechter. Dit geeft de burger – en organisaties waarin burgers zich verenigen – te weinig mogelijkheden om besluitvorming op basis van Big Data-processen te bevragen zolang zij geen gezamenlijke persoonlijke benadeling kunnen aanvoeren. Het is dus belangrijk dat de rechter selectief zaken toelaat die recht doen aan collectieve zorgen en bijdragen aan de *opbouw van jurisprudentie* op dit belangrijke en relatief onontgonnen terrein.