Excellenties,

U bent van plan om big data-analyses in te laten zetten door opsporings- en inlichtingendiensten en wilt daar beleid voor ontwikkelen. Ter voorbereiding hiervan is de Wetenschappelijke Raad voor het Regeringsbeleid (WRR) verzocht om advies uit te brengen. Naar aanleiding van het WRR-rapport 'Big Data in een vrije en veilige samenleving' nodigt u verschillende partijen uit voor een open gedachtewisseling over het rapport, met een specifieke nadruk op de implicaties voor het grondrecht op privacy bij het gebruik van big data in het veiligheidsdomein. Wij stellen deze mogelijkheid zeer op prijs en gaan graag in op uw uitnodiging.

Kort samengevat wijzen we erop dat de rechtsbescherming van de burger niet ondergeschikt mag worden gemaakt aan efficiencywinsten die de overheid met big data-toepassingen hoopt te behalen. In de volgende pagina's vindt u een verdere uitwerking van onze punten van zorg:

- **Ongerichte surveillance en gebrek aan doelbinding** – belangrijke uitgangspunten van de rechtsstaat worden hierdoor losgelaten.
- **Ontbreken van noodzaak** – de overheid kan door de ontwikkeling van technologische mogelijkheden niet ontslagen worden van haar plicht tot het aantonen van de noodzaak van iedere inbreuk op de privacy van de burger.
- **Schadelijke effecten binnen een democratische rechtsstaat:**
  - Vrije meningsuiting en zelfcensuur – burgers passen vaker zelfcensuur toe en de controlerende rol van de media op de staat komt in het geding.
  - Verstoring relatie tussen overheid en burger – door de toenemende asymmetrie in de informatiepositie van de overheid aan de ene kant en burgers aan de anderen kant.
  - Individuele rechtsbescherming in het gedrang – de burger zal straks moeten bewijzen ten onrechte met een profiel te zijn geassocieerd, in plaats van omgekeerd.
  - Vals positieven – juist in de publieke context zijn vals positieven maatschappelijk slecht te legitimeren.
  - Institutionele vooroordelen – datasets worden samengesteld door mensen met hun menselijke vooringenomenheid. In 'machine learning' omgevingen met de bijbehorende 'feedback loops', worden discriminatieproblemen cumulatief versterkt.
  - Vertrouwen in digitale communicatie wordt aangetast – als burgers de digitale infrastructuur niet meer kunnen vertrouwen, richt dat maatschappelijke schade aan.

Tijdens ons gesprek zullen we deze punten graag nader toelichten. Wij kijken uit naar uw reactie.

Hoogachtend,

Bits of Freedom
Hans de Zwart

Nederlandse Vereniging voor Strafrechtadvocaten (NVSA)
Brendan Newitt

Internet Society Nederland (ISOC)
Alexander Blom

Jaap-Henk Hoepman
Wetenschappelijk directeur Privacy & Identity Lab en universitair hoofddocent computersecurity, privacy en identitymanagement aan de Radboud Universiteit.

Nederlandse Vereniging van Journalisten (NVJ)
Thomas Bruning

PILP/NJCM (Nederlands Juristen Comité voor de Mensenrechten
Jelle Klaas

Privacy First
Vincent Böhre

Big data is niet nieuw
In dit document wordt voor de definitie van big data uitgegaan van dezelfde kenmerken als in het WRR-rapport[1]: grote hoeveelheden gestructureerde en ongestructureerde gegevens uit verschillende bronnen, waarop een 'data-driven' analyse wordt toegepast, er sprake is van een ontschotting van domeinen en er wordt door middel van correlationele verbanden gezocht naar 'actionable knowledge'. Het rapport stelt terecht dat dit geen nieuw fenomeen is.

We willen hierbij onderstrepen dat big data in dit domein geen abstract begrip is, maar gaat over mensen.

Twee fundamentele problemen: ongerichte surveillance en gebrek aan doelbinding
Het grote probleem bij big data-toepassingen in het veiligheidsdomein is dat een van de uitgangspunten van de rechtsstaat (geparafraseerd): 'een burger die niets verkeerd doet wordt niet in de gaten gehouden', wordt verlaten. Gerichte surveillance wordt losgelaten, gegevens van onverdachte burgers worden immers op grote schaal verzameld. Ook wordt doelbinding zowel tijdens het verzamelen als tijdens de analyse losgelaten.

Beide vormen een groot probleem met het mensenrechtelijk kader, meer specifiek gaat het voorbij aan het recht op respect voor het privéleven, zoals vastgelegd in artikel 8 EVRM. Iedere inbreuk op dit recht moet voldoen aan de vereisten die voortvloeien uit lid 2 van dit artikel. Het is dan ook onder andere vanwege de ongerichte surveillance dat het Europees Hof van Justitie de dataretentierichtlijn ongeldig heeft verklaard.[2] Wij verwachten daarom dat juist in het veiligheidsdomein het gebruik van big data-toepassingen in de nabije toekomst zou kunnen leiden tot rechtszaken bij het Europees Hof voor de Rechten van de Mens.

Ontbreken van noodzaak
De in het rapport geschetste kansen van gebruik van big data-toepassingen zijn niet overtuigend: niet alleen wordt er al direct een voorbehoud gemaakt ("mits het gebruik hiervan niet zelf een oorzaak van onveiligheid wordt"), ook liegen de geschetste beperkingen en met name de risico's er niet om.[3] Maar belangrijker, de noodzaak voor het gebruik van big data-toepassingen wordt nergens aangetoond.

Het is zeer zorgelijk dat het rapport feitelijk een vorm van technologisch determinisme herbergt, die het laten vieren van de teugels bij gegevensverzameling binnen big data als onvermijdelijk presenteert. Echter, de overheid kan niet ontslagen worden van haar plicht tot het aantonen van de noodzaak van iedere inbreuk op de privacy van de burger, enkel door de ontwikkeling van de technologische mogelijkheden. Er is geen reden om in het kader van de bescherming van burgerrechten big data als een exceptie te beschouwen. Als big data-toepassingen niet binnen de kaders van de huidige wet kunnen worden toegepast, moet niet de focus op andere beginselen komen te liggen, maar moeten de big data-toepassingen (zolang) niet of anders worden uitgevoerd.

Schadelijke effecten binnen een democratische rechtsstaat
Extra regulering van het gebruik van gegevens (zoals gesuggereerd in het WRR-rapport) mag niet afleiden van de regulering en handhaving van het verzamelen.

Vrije meningsuiting en zelfcensuur
Een deel van de negatieve maatschappelijke consequenties treedt op op het moment van (ongericht) verzamelen. Mensen die zich bekeken voelen, passen hun gedrag aan naar door hen als wenselijk gepercipieerd gedrag, het zogenaamde 'chilling effect'.[4] Dit effect treedt het sterkst op bij kwetsbare groepen.

---

[1] *WRR-rapport 'Big Data in een vrije en veilige samenleving'*, Amsterdam: Amsterdam University Press 2016, http://www.wrr.nl/fileadmin/nl/publicaties/PDF-Rapporten/rapport_95_Big_Data_in_een_vrije_en_veilige_samenleving.pdf.

[2] Zie bijvoorbeeld overwegingen 57 t/m 59 HvJ EU in de gevoegde zaken C 293 12 en C 594 12 over de dataretentierichtlijn (2006/24/EG), https://www.bof.nl/live/wp-content/uploads/c_293_c_594.pdf.

[3] WRR-rapport, p. 132 en 134.

[4] Zie J. Penney, *Chilling Effects: Online Surveillance and Wikipedia Use*, SSRN: http://ssrn.com/abstract=2769645 en A. Marthews en C. Tucker, *Government Surveillance and Internet Search Behavior*, SSRN: http://ssrn.com/abstract=2412564.

Het WRR-rapport concludeert daarnaast terecht dat een controlerende rol van de media op de staat daarmee ook in het geding komt wanneer journalisten en redacties dit soort gedrag gaan vertonen. Dit brengt ons in een gelijke positie met landen die weinig hechten aan de grondbeginselen van een democratische rechtsstaat, waaronder vrije media en het recht op informatie..

Verstoring relatie tussen overheid en burger

Het verzamelen van gegevens over burgers verstoort de machtsbalans tussen de overheid en haar burgers. Big data-toepassingen in het veiligheidsdomein vergroten dat effect. De toegenomen informatie-assymmetrie komt door het feit dat de kostenbarrière tegen overheidsinmenging verlaagd wordt. De overheid kan een keer iets doen, en vervolgens een miljoen keer hetzelfde doen zonder extra kosten. Onderwijl komt zij steeds verder in de private levenssfeer van de individuele burger. Deze kan echter steeds slechter voorzien wat er gebeurt met zijn gegevens en wat daarvan de consequenties zijn.

Individuele rechtsbescherming in het gedrang

De WRR noemt terecht het gevaar van omkering van de bewijslast bij surveillance, handhaving en fraudebestrijding. Het gevaar is dat bij geschillen de bewijslast bij de burger komt te liggen. Die moet dan bewijzen ten onrechte met een profiel te zijn geassocieerd, in plaats van omgekeerd.

Vals positieven

Bij het plaatsen van mensen in hokjes op basis van big data zullen er per definitie vals positieven optreden: mensen die onterecht een bepaald label opgeplakt krijgen. Het WRR-rapport geeft helder aan dat bij een data-zoektocht naar zaken die heel weinig voorkomen (zoals terrorisme) het aantal vals positieven te groot wordt.[5] Onterechte surveillance, tapbevelen of zelfs huisbezoeken zijn bijzonder kwalijk. Juist in de publieke context zijn vals positieven maatschappelijk slecht te legitimeren en moeten zoveel mogelijk vermeden worden.[6]

Institutionele vooroordelen worden versterkt

Het gebruik van big data-toepassingen kan leiden tot (indirecte) discriminatie. Dat komt doordat in de verzameling van data en de keuze voor datasets vaak al een vooringenomenheid schuilgaat. Data zijn, net zo min als algoritmes, neutraal – ze worden samengesteld door mensen met hun menselijke vooroordelen. Zeker in 'machine learning' omgevingen met de bijbehorende 'feedback loops', is dat een probleem. Huidige discriminatieproblemen zullen daardoor cumulatief versterkt worden.[7]

Vertrouwen in digitale infrastructuur wordt aangetast

We onderstrepen het belang van een internet dat vrij door eenieder op anonieme basis betreden kan worden, en waar politiek, sociaal verkeer en commercie hun plek hebben. Als de inzet van big data-toepassingen tot gevolg heeft dat burgers hun vertrouwen verliezen in de digitale infrastructuur, omdat ze zich realiseren dat

---

[5] Zie WRR-rapport, p. 132: "*Datamining – de voor Big Data kenmerkende analysevorm – is niet voor alle vormen van misdaadbestrijding even geschikt. Datamining is voor het voorkomen van terroristische aanslagen waarschijnlijk een ineffectieve methode. Patroonherkenning werkt het beste bij overtredingen die een vast en terugkerend patroon laten zien. Omdat elke terroristische aanslag uniek is, is het nagenoeg onmogelijk om een goed profiel te maken. In combinatie met een gering aantal aanslagen levert dit te hoge foutpercentages op.*"

[6] Zie de statistieken van het CBS van 2004 tot 2015 over uitgekeerde schadevergoedingen voor onterechte hechtenis of onterecht gemaakte kosten: https://www.cbs.nl/nl-nl/nieuws/2016/16/meer-schadevergoedingen-naar-ex-verdachten.

[7] Zie recent onderzoek van ProPublica over Machine Bias bij rechtspraak in de Verenigde Staten: https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing. Zie ook Managing 'Threats': Uses of Social Media for Policing Domestic Extremism and Disorder in the UK: "*Rather, big data is predominantly used to identify patterns that are subjectively (humanly) interpreted and assessed, not least in the identification of any anomalies within these patterns. Thus, discretion (and as outlined in our background section, assumptions and ideology) is a key feature in data-driven policing. In particular, pre-existing knowledge, intelligence and broader societal understandings of events continue to shape and determine big data analyses. Whilst this helps correct the imperfections of the technology, it opens up possibilities for pre- existing human biases to enter predictive policing, resulting in the discriminatory implications that several researchers have highlighted*", http://www.dcssproject.net/files/2015/12/Managing-Threats-Project-Report.pdf.

hun gedrag automatisch wordt geanalyseerd en die analyses door de overheid worden gebruikt, heeft dat nadelige democratische, sociale en economische consequenties.

Aanbevelingen naar aanleiding van het WRR-rapport

Houd focus op het reguleren van het verzamelen van gegevens
De nadruk op minimaliseren van het verzamelen van gegevens moet worden vastgehouden. Immers, alleen bij de verzameling heeft de burger inzicht in welke gegevens verzameld kunnen worden, bij het verwerken is dat er niet meer. Dit betekent dat de verzameling al hypothese-gedreven moet zijn en dat er sprake moet blijven van doelbinding.

Beperk het gebruik van niet verklaarbare correlaties
Correlaties die niet door mensen (dus deductief) te verklaren zijn, zouden niet gebruikt mogen worden in het veiligheidsdomein. De nadruk zou daarentegen moeten liggen op hypothese-gedreven data-analyses en verklaarbare voorspellingen.

Breng balans in relatie tussen overheid en burger
Het WRR-rapport omschrijft dat in reactie op de groeiende informatie-asymmetrie tussen de overheid en de burger, de laatste meer toetsingsmogelijkheden dient te krijgen op overheidsbeslissingen die haar aangaan.[8] Het maakt helaas niet duidelijk hoe dit concreet bewerkstelligd moet worden, zeker wanneer het 'geheime' informatie betreft zoals bij het werk dat inlichtingendiensten verrichten.

We ondersteunen de oproep van de WRR om de positie van NGO's en burgerrechtenorganisaties te versterken en te verstevigen in juridische procedures ter toetsing van big data-toepassingen.[9] Daarbij moet er echter geen sprake zijn van "selectieve ontvankelijkheid"[10] , aangezien dat tot willekeur zal leiden. De laatste jaren staat de ontvankelijkheid van belangenorganisaties om in het algemeen belang te procederen in toenemende mate onder druk. Wij pleiten daarom in lijn met de conclusies van het WRR-rapport voor het herstel en de versterking van de civielrechtelijke algemeen-belangactie onder artikel 3:305a BW en voor de mogelijkheid van rechterlijke toetsing aan de Grondwet.

Een ander belangrijke vereiste voor het versterken van tegenkrachten is dat toezichthouders zoals de Autoriteit Persoonsgegevens en de Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (CTIVD) hun technische en datawetenschappelijke capaciteit en expertise kunnen versterken.

Wat is de impact van het WRR-rapport op de huidige situatie en wetsvoorstellen?
Het baart ons zorgen dat er zo voorspoedig over big data-toepassingen in big data-pilots in het veiligheidsdomein wordt nagedacht, terwijl de Nederlandse overheid haar data-huishouden nog niet helemaal op orde heeft.

Zo overtreedt de politie al meer dan zeven jaar grote delen van de Wet politiegegevens, die bepaalt hoe zij met gegevens van burgers om moet gaan. De Minister van Veiligheid en Justitie heeft aangegeven dat deze situatie voorlopig niet zal veranderen. Dat is een zorgelijke uitgangspositie voor de inzet van big data-toepassingen.

Tot slot zijn we benieuwd hoe de verantwoordelijke ministers de aanbevelingen in het rapport zien in het licht van actuele wetsvoorstellen, zoals met name de herziening van de Wet op de inlichtingen- en veiligheidsdiensten.

---

[8] WRR-rapport, p. 143.

[9] WRR-rapport, p. 122 en 146.

[10] WRR-rapport, p. 146.