Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2016–2017

26 643 Informatie- en communicatietechnologie (ICT)

32 761 Verwerking en bescherming persoonsgegevens

Nr. 426

BRIEF VAN DE MINISTER VAN VEILIGHEID EN JUSTITIE

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 11 november 2016

1. Inleiding

Op 28 april jl. heeft de Wetenschappelijke Raad voor het Regeringsbeleid (WRR) het kabinet het rapport «Big Data in een vrije en veilige samenleving» aangeboden. Met dit rapport geeft de WRR zijn reactie op de adviesaanvraag van het kabinet over het thema «Big data, veiligheid en privacy» van 26 mei 2014. Deze adviesaanvraag kwam voort uit de notitie «Vrijheid en veiligheid in de digitale samenleving. Een agenda voor de toekomst» die het kabinet op 13 december 2013 aan de Kamer heeft gezonden.[1]

Het kabinet heeft met veel waardering van het rapport kennis genomen. De WRR constateert naar het oordeel van het kabinet op goede gronden dat Big Data een belangrijke bijdrage kan leveren aan het bevorderen van de veiligheid. Hij wijst ook terecht op de risico's die met Big Data toepassingen gepaard kunnen gaan. Met het oog op deze risico's formuleert de WRR een regulerend kader voor de analyse en het gebruik van Big Data en bepleit hij een versteviging van het toezicht, de transparantie en de rechterlijke toetsing met betrekking tot de analyse van Big Data en het gebruik daarvan.

In deze brief geeft het kabinet op hoofdlijnen zijn reactie op het rapport van de WRR. De kernboodschap van het kabinet in deze reactie is:

> Big Data biedt veel kansen om de veiligheid te bevorderen. Om deze kansen te benutten dient er voldoende ruimte te zijn om de toegevoegde waarde van Big Data verder te verkennen. Big Data laat ook risico's zien. Daarom zal het experimenteren en benutten van Big Data gepaard moeten gaan met voldoende waarborgen waarin bescherming van de privacy en persoonsgegevens, het verbod van discriminatie, transparantie en de betrouwbaarheid van zowel data

[1] Kamerstuk 26 643, nr. 298.

kst-26643-426
ISSN 0921 - 7371
's-Gravenhage 2016

als analysemethoden centraal staan. Zo kan worden bereikt dat er voldoende vertrouwen bij de burgers bestaat in de wijze waarop de overheid de mogelijkheden van Big Data in het veiligheidsdomein benut.

Hoewel dit rapport zich hoofdzakelijk op het veiligheidsdomein richt, meent het kabinet er goed aan te doen hierna in § 2 eerst kort de ontwikkelingen rond Big Data op andere terreinen aan te stippen. Vervolgens staat het kabinet in § 3 stil bij de analyse van de WRR. Daarna formuleert het in § 4 in reactie op de aanbevelingen van de WRR een aantal beleidsuitgangspunten en actiepunten met betrekking tot Big Data op het terrein van de veiligheid. In een bijlage bij de brief gaat het kabinet meer specifiek op onderdelen van de analyse en op de verschillende aanbevelingen uit het rapport in. In deze brief en de bijlage[2] betrekt het kabinet ook punten die de Privacycoalitie in een gesprek met leden van het kabinet over het rapport naar voren heeft gebracht.[3]

2. Context

Wat precies onder Big Data moet worden verstaan, is volgens de WRR niet eenduidig. De Raad zelf hanteert voor de duiding van het begrip «Big Data» een drietal hoofdkenmerken:

1. *Data*: het gaat om grote hoeveelheden gestructureerde en ongestructureerde data uit verschillende bronnen.
2. *Analyse*: de analyse is *data driven*, zoekt geautomatiseerd naar correlaties en heeft vooral potentie voor analyses van het heden (*realtime analysis*) en de toekomst (*predictive analysis*).
3. *Gebruik*: de analyses moeten leiden tot *actionable knowledge*, kennis om te kunnen toepassen voor beslissingen op groeps- of individueel niveau.

Het kabinet kan zich in deze hoofdkenmerken in beginsel goed vinden met dien verstande dat het ook de feitelijke toepassing van de kennis uit Big Data analyses op personen of groepen in zijn beschouwingen zal betrekken.

Het rapport van de WRR richt zich hoofdzakelijk op Big Data binnen het veiligheidsdomein en daarmee vooral op wat de Raad zelf ooit de controletaak van de overheid heeft genoemd.[4] Daarvan zijn te onderscheiden de dienstverlenende taak en de zorgtaak van de overheid. Big Data biedt de overheid bij de uitvoering van die laatste twee taken kansen om burgers effectiever en efficiënter te bedienen, bijvoorbeeld door meer maatwerk in de dienstverlening en zorg aan burgers. Op het terrein van de sociale zekerheid is dit van belang voor het UWV, de SVB en gemeenten. Ook op het terrein van onderwijs, cultuur en wetenschap biedt het gebruik van Big Data kansen.[5] In lijn met het rapport van de WRR richt het beleid van het kabinet voor de verwerking van gegevens bij het uitvoeren van de dienstverlenende taken van de overheid zich steeds meer op het reguleren van het gebruik van gegevens dan enkel op het inwinnen of beheren van gegevens. In dat kader legt het kabinet in bindende bestuurlijke afspraken de uitgangspunten voor de vereiste kwaliteit, transparantie en toeganke-

[2] Raadpleegbaar via www.tweedekamer.nl

[3] De Privacycoalitie is een verband van – aanvankelijk – 32 organisaties, bedrijven en personen dat in een open brief van 2 april 2015 zorgen heeft geuit over de privacybescherming van burgers in onze informatiemaatschappij. In zijn reactie op die brief heeft de Minister van Veiligheid en Justitie toegezegd bij het opstellen van een kabinetsstandpunt over het advies van de WRR ook de inbreng van de Privacycoalitie te betrekken (Kamerstuk 32 761, nr. 83, blz. 4).

[4] Wetenschappelijke Raad voor het Regeringsbeleid, iOverheid, 2011, blz. 72.

[5] Zie de brief van de Minister van Onderwijs, Cultuur en Wetenschappen van 28 juni 2016 aan de Tweede Kamer (Kamerstuk 31 288, nr. 545).

lijkheid van gegevens vast.[6] Daarnaast komt het kabinet zo nodig met voorstellen voor nieuwe regelgeving om een juist gebruik van gegevens ten behoeve van een betere dienstverlening te bevorderen en een stevigere regie op gegevens voor burger en ondernemer mogelijk te maken.[7]

Big Data speelt ook een grote rol in de particuliere sector. Het kabinet heeft in zijn brief van 19 november 2014 een aanzet gegeven tot een kabinetsvisie op Big Data, profilering en privacy in de private sector.[8] In vervolg hierop heeft het kabinet op 5 oktober jl. het rapport van de expertgroep Big Data en privacy aan de Tweede Kamer aangeboden met een reactie op de bevindingen van de expertgroep.[9] Ook dat rapport heeft primair betrekking op het gebruik van Big Data door het bedrijfsleven.

Het onderhavige kabinetsstandpunt concentreert zich op de overheid in haar rol van gebruiker van Big Data ten behoeve van het borgen van de veiligheid.

3. Analyse

Veiligheid en Big Data

De overheid heeft – zo stelt de WRR terecht – de plicht om haar burgers te beschermen en de veiligheid te vergroten om ervoor te zorgen dat zij in vrijheid kunnen leven. De overheid moet daarom zorgdragen voor de maatschappelijke en individuele veiligheid, onder meer door informatie in te winnen, waakzaam te zijn en bronnen van onveiligheid te bestrijden. Hierbij moet de overheid voldoende afstand houden van het persoonlijke leven van de burger. Het veiligheidsbeleid moet zo zijn ingekaderd dat het zowel de persoonlijke als de maatschappelijke vrijheid beschermt.

Met het oog op de informatiepositie van de overheid op het terrein van de veiligheid is het van belang dat de hoeveelheid beschikbare data de laatste jaren enorm is toegenomen en met grote snelheid verder zal groeien.[10] De oorzaak daarvan ligt vooral in het feit dat veel data tegenwoordig automatisch worden geproduceerd en het bijproduct zijn van het gebruik van internet, social media, mobiele telefoons en applicaties. Bovendien verdubbelt de opslagcapaciteit ongeveer iedere drie jaar en nemen de kosten van dataopslag sterk af, waardoor er een opwaartse druk op het bewaren van data is ontstaan. Door het koppelen van databases, het gebruik van steeds krachtigere computers, betere software en algoritmen en *machine learning* wordt het mogelijk om uit deze groeiende hoeveelheid data veel sneller dan voorheen nieuwe kennis te construeren. Deze ontwikkelingen hebben geleid tot het fenomeen Big Data, zoals dat hiervóór in § 2 is geduid.

De enorme groei van de hoeveelheid data en de ontwikkeling van allerlei geavanceerde analysetechnieken om daar informatie uit te halen brengen overigens mee dat naast de overheid ook andere partijen in toenemende mate over informatie beschikken die binnen het veiligheidsdomein van belang kan zijn. Denk aan informatie die kan worden gegenereerd door

---

[6] Zie het Digiprogramma 2016–2017 dat op 31 maart 2016 aan de Tweede Kamer werd aangeboden (Kamerstuk 26 643, nr. 402).

[7] Zie https://www.digicommissaris.nl/page/890/digiprogramma-2016–2017-aangeboden-aan-tweede-kamer.

[8] Kamerstuk 32 761, nr. 78.

[9] Kamerstuk 32 761, nr. 108.

[10] De WRR verwijst in dit verband naar een schatting van IDC uit 2014 waarin naar voren komt dat de hoeveelheid opgeslagen data tussen 2013 en 2020 groeit van 4,4 zettabytes (een zettabyte is 10^{21}bytes) naar 44 zettabytes, meer dan een verdubbeling per twee jaar.

applicaties voor social media monitoring of informatie over de veiligheid in een wijk op buurtapps. Soms komt dergelijke informatie tijdig ook bij de overheid terecht, maar soms ook niet. Dit leidt ertoe dat de overheid in sterkere mate dan voorheen het verwijt kan krijgen dat zij op het terrein van de veiligheid iets niet heeft gedaan of iets niet heeft voorkomen, terwijl er wel informatie was die aanleiding tot actie zou hebben gegeven. Dit pleit er uiteraard niet voor om de overheid dan maar alle ruimte te geven om data en informatie te verzamelen, maar impliceert wel dat de overheid burgers duidelijk moet maken welke afwegingen zij maakt om bepaalde data en informatie te kunnen en mogen gebruiken en wat de overheid als gevolg van deze afwegingen wel en niet aan veiligheid kan bieden. Overigens zal de overheid er uiteraard altijd naar streven om, binnen de grenzen van haar wettelijke bevoegdheden, in de samenleving beschikbare informatie ten behoeve van de veiligheid te benutten.

Kansen Big Data

Evenals de WRR is het kabinet van oordeel dat Big Data analyses kunnen bijdragen aan een efficiënter en effectiever gebruik van data door politie, justitie, de inlichtingen- en veiligheidsdiensten en andere organisaties binnen het brede veiligheidsdomein. De veiligheid in ons land kan daardoor worden bevorderd. Een aantal overheidsorganisaties is dan ook al begonnen met Big Data (proef)projecten. De WRR noemt daarvan in zijn rapport een aantal voorbeelden, zoals de politie, de Belastingdienst en de inlichtingen- en veiligheidsdiensten. Het kabinet wijst zelf nog op de oprichting van een broedkamer (Living Lab) waarin experimenten met Big Data op het terrein van de veiligheid worden uitgevoerd.[11] De oprichting daarvan wordt ingegeven door de gedachte dat de overheid met betrekking tot Big Data vooral een lerende overheid dient te zijn die binnen de wettelijke kaders en met toepassing van het concept van «Privacy by Design» experimenten uitvoert en daarbij gebruik maakt van kennis die elders al is ontwikkeld.

Als we wat nauwkeuriger naar de kansen van Big Data kijken, zien we dat met behulp van Big Data analyses bijvoorbeeld inschattingen kunnen worden gemaakt van mogelijke risico's om tijdig preventieve maatregelen te kunnen treffen, de modus operandi van criminelen inzichtelijk kan worden gemaakt, *realtime* ontwikkelingen in crisissituaties kunnen worden gevolgd of *crowd control* rond evenementen kan worden uitgevoerd. Daarbij kunnen inzichten ontstaan die met meer traditionele middelen niet of pas na veel meer tijdsverloop ontwikkeld kunnen worden. Big Data biedt ook de kans op meer objectieve analyses dan met behulp van de kennis van experts mogelijk is. Verder is van belang dat criminaliteit zich in toenemende mate in de virtuele wereld afspeelt. Dit leidt tot verdere proliferatie van digitale data, die tot de inzet van steeds slimmere zoekmachines noopt. Big Data analyses zijn in dat verband onmisbaar. Tegen deze achtergrond heeft het kabinet voor ogen dat er voldoende ruimte moet zijn om de toegevoegde waarde van Big Data verder te verkennen.

Op dit moment vinden reeds Big Data toepassingen plaats die goede resultaten laten zien. Zo gebruikt de politie een forensische zoekmachine om grote hoeveelheden gegevens afkomstig van in beslaggenomen gegevensdragers binnen enkele uren te onderzoeken en te ordenen, waar dit vroeger vele dagen in beslag nam. De politie maakt verder voor specifieke thema's binnen de opsporing van zware criminaliteit, zoals liquidatieonderzoeken en contraterrorisme, gebruik van moderne analysetools waarmee gestructureerde en ongestructureerde data uit

[11] Kamerstuk 29 279, nr. 298, blz. 3.

diverse politiesystemen in samenhang worden geanalyseerd. Met «Dynamisch Monitoren» hanteert de Belastingdienst een techniek waarmee al in een vroeg stadium een koppeling wordt gelegd tussen openstaande vorderingen en concrete verhaalsmogelijkheden, waardoor zowel nieuwe verhaalsmogelijkheden ontstaan als maatwerk voor de belastingplichtige kan worden geleverd. Tot slot vermelden wij hier het project FinPro waarbinnen onderzoeken zijn uitgevoerd naar de mogelijkheden van het combineren van data uit zeer diverse bronnen voor het inzichtelijk maken van fraude en ondermijnende criminaliteit.[12] In de bijlage bij deze brief worden deze en andere voorbeelden verder toegelicht[13].

Risico's Big Data

De verschillende kansen die Big Data biedt, mogen de ogen intussen niet doen sluiten voor de risico's die aan Big Data analyses zijn verbonden. In het veiligheidsdomein blijft het maken van de juiste afwegingen binnen de juridische kaders voor de bescherming van de persoonlijke levenssfeer en van persoonsgegevens cruciaal. De WRR en de Privacycoalitie wijzen er in dit verband op dat Big Data toepassingen per definitie gepaard gaan met de verzameling, opslag en analyse van grote hoeveelheden data, waardoor de beginselen van noodzakelijkheid en proportionaliteit uit het gegevensbeschermingsrecht onder druk komen te staan en zich het risico kan voordoen dat er *chilling effects* (inperkende effecten) optreden met betrekking tot diverse grondrechten, waaronder de vrijheid van meningsuiting, bescherming tegen discriminatie en het recht op een eerlijk proces. Volgens de WRR zijn Big Data toepassingen ook gevoelig voor *function creep* (de «sluipende» uitbreiding van doelen waarvoor data worden verwerkt) waardoor strijd met het principe van doelbinding kan ontstaan. De WRR maakt zich verder zorgen over het toenemende gebrek aan transparantie rond Big Data toepassingen en de daarbij gebruikte profielen, algoritmen en methoden. Ook wijst de Raad evenals de Privacycoalitie op het risico dat dergelijke toepassingen een onevenredige sociale impact hebben door onregelmatigheden in de gebruikte datasets en algoritmen. Zonder correctie kan zich dit op termijn in een cumulatief nadeel voor bepaalde groepen in de maatschappij vertalen in de vorm van bijvoorbeeld discriminatie. Tegen de achtergrond van deze overwegingen is het kabinet van oordeel dat de verdere ontwikkeling van het gebruik van Big Data niet anders zou moeten plaatsvinden dan met de gelijktijdige ontwikkeling van effectieve waarborgen om risico's, zoals de WRR en de Privacycoalitie die constateren, in passende mate te beperken.

De hier bedoelde waarborgen raken de ethische kant van het gebruik van Big Data. Voor het kabinet staan hierin bescherming van de privacy, bescherming van persoonsgegevens, het verbod van discriminatie, transparantie en betrouwbaarheid van zowel data als analysemethoden centraal. Alleen als aan deze aspecten voldoende aandacht wordt geschonken, die aandacht uitmondt in effectieve waarborgen en deze waarborgen op de juiste wijze worden toegepast, kan er een duurzaam vertrouwen bestaan bij de burgers in de wijze waarop de overheid Big Data benut bij de uitvoering van haar taken. Het beleid dat het kabinet op dit punt wil voeren, komt hierna in § 4 van deze brief aan de orde. Daarbij heeft het kabinet rekening gehouden met het gegeven dat het met het oog op het grote belang van een adequate bestrijding van fraude en criminaliteit contraproductief kan zijn om algehele openheid van zaken tegenover burgers te geven over risicoselectiecriteria, algoritmen en analysemethoden die uitvoeringsorganisaties en toezichthouders hanteren bij de

[12] Aanhangsel Handelingen II 2016/17, nr. 3413.
[13] Raadpleegbaar via www.tweedekamer.nl

inrichting van hun (controle)processen. In hoeverre vanuit deze optiek openheid mogelijk is moet nog nader worden onderzocht.

Aan het vertrouwen dat burgers hebben in het gebruik van Big Data, kan verder worden bijgedragen door met relevante partijen voortdurend in dialoog te blijven over de wijze waarop de overheid deze kansen wil benutten, en over de normen en principes die zij daarbij hanteert, zeker nu niet alle mogelijke gevolgen van Big Data vooraf zijn te overzien, laat staan te doordenken. Voor een dergelijke dialoog is ook aanleiding, omdat de verwerking van Big Data in het veiligheidsdomein een proces is waarin niet alleen individuele grondrechten een rol behoeven te spelen. Vanwege het volume van de betrokken data en daarmee het aantal betrokken personen kan van een potentiële impact op de samenleving sprake zijn die rechtvaardigt dat bescherming van de privacy in voorkomende gevallen ook als een collectieve waarde wordt gezien. Het kabinet meent dat het in dergelijke gevallen wenselijk is dat het belang van deze collectieve waarde ook op collectief niveau wordt behartigd. Het wil dan ook graag de dialoog versterken met organisaties die het privacybelang behartigen. Versterking daarvan zou aansluiten bij de opvatting van de Privacycoalitie dat de burger steeds slechter kan voorzien wat er gebeurt met zijn gegevens en wat daarvan de consequenties zijn.

Het verrichten van Big Data analyses kan verschillende gevolgen hebben voor de personen van wie gegevens worden verwerkt. Dit kunnen enerzijds *directe* gevolgen zijn, bijvoorbeeld wanneer personen of groepen passen in een profiel en er op basis daarvan richting die personen concrete stappen worden gezet. Dit kunnen overigens positieve stappen zijn, bijvoorbeeld wanneer iemand door de politie wordt gewaarschuwd dat er een verhoogd risico is op inbraak in zijn wijk. Maar het kunnen ook gevolgen zijn die voor betrokkene ongewenst zijn. Bijvoorbeeld wanneer men past in een profiel en op basis daarvan gericht meer controles worden uitgeoefend op een persoon of onderneming.

Naast deze *directe* gevolgen is het mogelijk dat er meer *indirecte* gevolgen optreden naar aanleiding van Big Data analyses. Daarbij valt primair te denken aan de eerder al genoemde *chilling effects.* Dat houdt in dat personen hun normale, volstrekt legale gedrag aanpassen omdat zij bang zijn dat zij anders nadelige gevolgen kunnen ondervinden. Een voorbeeld: het lezen van bepaalde kranten en het bezoeken van bepaalde websites kan als relevant kenmerk meegewogen worden in een Big Data analyse. Dit kan bijdragen aan de (geautomatiseerde) conclusie dat er een verhoogd risico is op ongewenst gedrag, zoals radicalisering of het plegen van strafbare feiten, terwijl daar in werkelijkheid geen sprake van hoeft te zijn. Het indirecte gevolg kan dan zijn dat burgers, ook degenen die zich aan de wet houden, zich calculerend opstellen, bijvoorbeeld door hun mening minder vrij te uiten, minder vrijelijk informatie op te zoeken op het internet of minder digitaal met elkaar te communiceren omdat het potentieel leidt tot benadeling, ook al is het niet bij wet verboden. Ter voorkoming van het ontstaan van dergelijke indirecte gevolgen worden waarborgen aangebracht ten aanzien van overheidsoptreden binnen het veiligheidsdomein op basis van Big Data analyses. Te denken valt in ieder geval aan de elders in deze brief en in de bijlage beschreven gevallen waarin menselijke tussenkomst bij beslissingen over overheidsoptreden binnen dat domein op zijn plaats is.

Naar versterking van het kader voor analyse en gebruik van Big Data

In navolging van de WRR wijst het kabinet er aan het slot van deze paragraaf op dat de huidige juridische kaders voor gegevensverwerking binnen het veiligheidsdomein vooral gericht zijn op het *verzamelen* van

gegevens. Het kabinet is met de Raad van oordeel dat de eisen aan het verzamelen van gegevens een belangrijke functie hebben, maar ook dat het verzwaren van deze eisen niet de aangewezen weg vormt om de risico's met betrekking tot Big Data te mitigeren. Dat zou een groot deel van de belofte van Big Data in de kiem smoren. Het kabinet is het dan ook eens met de opvatting van de Raad dat beter kan worden ingezet op versterking van de regulering van de fases waarin de *analyse* en het *gebruik* van Big Data plaatsvinden. Het vat regulering daarbij zo op dat het kan gaan om een mix van wettelijke voorschriften en uitgangspunten voor het beleid dat de rijksoverheid voert.

4. Beleidsuitgangspunten en actiepunten

De WRR doet verschillende aanbevelingen om het door hem bepleite regulatieve kader in te vullen. Het kabinet stelt graag voorop dat de bestaande regels voor verwerking van persoonsgegevens[14] en het hierna te noemen toekomstige Europese kader uiteraard ook gelden voor de verwerking van persoonsgegevens bij het gebruik van Big Data. Het stelt verder vast dat sommige aanbevelingen samenhang vertonen met voorschriften in de nieuwe Algemene verordening gegevensbescherming (AVG)[15] en de Richtlijn gegevensbescherming opsporing en vervolging[16]. Voor zover het om aanbevelingen gaat die al één op één hun vertaling in deze voorschriften vinden, neemt het kabinet deze uiteraard graag over. Als het echter aanbevelingen betreft die het beschermingsniveau van genoemde EU-regelingen te boven gaan, neemt het kabinet als uitgangspunt dat de aanbevelingen moeten worden beschouwd tegen de achtergrond van het – soms hogere – beschermingsniveau op basis van de geldende wet- en regelgeving op het gebied van de bescherming van persoonsgegevens in Nederland.

Beleidsuitgangspunten

In de bijlage[17] bij deze brief geeft het kabinet zijn reactie op elk van de aanbevelingen van de Raad. Deze reactie laat zich samenvatten in de volgende uitgangspunten voor het kabinetsbeleid met betrekking tot Big Data in het veiligheidsdomein, waarbij het kabinet aantekent dat sommige van deze beleidsuitgangspunten ook betekenis kunnen hebben voor andere domeinen:

- *Patroonherkenning (aanbeveling 1 in § 6.4.1).* De overheid zal Big Data in het veiligheidsdomein in de eerste plaats gebruiken voor de analyse van vraagstukken die zich goed voor patroonherkenning lenen, d.w.z. vraagstukken met een regelmatig en terugkerend karakter. Naarmate de mogelijkheden van patroonherkenning minder zijn, neemt het belang toe van een goede validatie door experts op het desbetreffende vakgebied om het risico op foutieve uitkomsten van de analyse zoveel mogelijk te reduceren.
- *Gebruik voor preventie (aanbeveling 2 in § 6.4.1).* Uitkomsten van Big Data analyses door de overheid zullen in het kader van preventie in beginsel ook kunnen worden gedeeld met burgers, private organisaties en bedrijven. Wel zal steeds per geval een risico-afweging moeten worden gemaakt die ertoe kan leiden dat niet de resultaten van de analyse zelf openbaar worden gemaakt, maar wel dat op basis van die

[14] Zie onder meer de Wet bescherming persoonsgegevens, de Wet politiegegevens en de Wet justitiële en strafvorderlijke gegevens.
[15] Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016, Pb L 119/1.
[16] Richtlijn (EU) 2016/680 van het Europees Parlement en de Raad van 27 april 2016, Pb L 119/89.
[17] Raadpleegbaar via www.tweedekamer.nl

resultaten in overleg met burgers en bedrijfsleven preventieve maatregelen worden getroffen.

- *Zorgplicht (aanbeveling 1 in § 6.4.4).* Overheidsdiensten zullen overeenkomstig de AVG en de Richtlijn ervoor moeten zorgen dat hun gegevens zoveel als met een redelijke inspanning mogelijk is *up to date* zijn en hun datasets een zo gering mogelijke *bias* (afwijking) bevatten, dat de door hen gebruikte algoritmen en analysemethoden deugdelijk zijn.
- *Reviews en toetsing (aanbeveling 2 in § 6.4.4).* Voor het uitvoeren van reviews op Big Data projecten en toepassingen volstaat het stelsel van gegevensbeschermingseffectbeoordelingen en toetsing van de verwerking dat is neergelegd in de AVG en de Richtlijn.
- *Evaluatie (aanbeveling 3 in § 6.4.4).* Bij Big Data projecten wordt voor een multidisciplinaire aanpak gekozen waarin stap voor stap naar een resultaat wordt toegewerkt. Een dergelijke aanpak impliceert dat doorlopend evaluaties van de behaalde resultaten plaatsvinden, met dien verstande dat grote dataverwerkingsprojecten vanwege het inrichten van een data infrastructuur, een data architectuur en het op sterkte krijgen van de benodigde Big Data expertise een doorlooptijd nodig kunnen hebben van één tot enkele jaren. Bij deze evaluaties zullen de behaalde resultaten nadrukkelijk moeten worden afgewogen tegen het belang van bescherming van persoonsgegevens.
- *Toelaatbare foutmarges (aanbeveling 1 in § 6.4.5).* De grootte van wat bij *profiling* als toelaatbare foutmarges wordt gehanteerd, kan slechts per geval of categorieën van gevallen worden bepaald. Betrokken partijen dienen deze foutmarges zoveel mogelijk voor een ieder transparant en bespreekbaar te maken. Controle op die foutmarges, de gebruikte methodes en de consequentie daarvan is essentieel teneinde het risico van fouten en een ondeugdelijke interpretatie van een profiel jegens een persoon of groep zo klein mogelijk te laten zijn.
- *Menselijke tussenkomst (aanbeveling 1 in § 6.4.5).* Op grond van de AVG en de Richtlijn geldt in beginsel een verbod op geautomatiseerde besluitvorming waaraan rechtsgevolgen zijn verbonden of die betrokkene anderszins in aanmerkelijke mate treft. Hierop zijn overigens wel (bij wet te maken) uitzonderingen mogelijk. Ook buiten situaties waarvoor dit verbod geldt, zal er binnen het veiligheidsdomein aanleiding kunnen zijn voor menselijke validatie van de analyse of nadere weging van de uitkomst daarvan, voordat op basis van deze analyse tot een beslissing wordt gekomen. Relevante criteria voor beantwoording van de vraag of daartoe aanleiding bestaat, zijn in elk geval de impact van het vervolg op burgers en het acute karakter of de ernst van de situatie waarop de analyse betrekking heeft.
- *Aantonen logica (aanbeveling 2 in § 6.4.5).* Overheidsdiensten zullen overeenkomstig de AVG en de Richtlijn dienen te zorgen voor rechtmatige en behoorlijke («eerlijke») Big Data processen. Zij zullen conform de AVG desgewenst informatie over de onderliggende logica van deze processen moeten verschaffen.
- *Transparantie (aanbeveling 1 in § 6.5).* De transparantie rond Big Data analyses en het gebruik daarvan moet waar mogelijk worden vergroot. Uitgangspunten en actiepunten, zoals elders in deze brief verwoord, kunnen hieraan bijdragen. Te denken valt aan transparantie van toelaatbare foutmarges, informatie over de gehanteerde logica achter Big Data processen en informatie over het doel van Big Data analyses en de daarvoor gebruikte databestanden. De transparantie dient beperkt te blijven, voor zover zij de effectiviteit van het gebruik van de uitkomsten van dergelijke analyses nadelig zou beïnvloeden.

Actiepunten

Tegen de achtergrond van de reactie die het kabinet in de bijlage[18] bij deze brief op de verschillende conclusies en aanbevelingen van de WRR geeft, formuleert het ook de volgende actiepunten:

- *Heldere wettelijke basis (§ 5.6.2).* Het kabinet zal bezien of de wettelijke basis voor het uitvoeren en gebruiken van data-analyses versterking behoeft, met inbegrip van de waarborgen die daarbij gehanteerd dienen te worden.
- *Inzicht in algoritmen (aanbeveling 1 in § 6.4.4).* Het kabinet zal onderzoeken hoe, rekening houdend met alle relevante belangen, voor toezicht en rechterlijke toetsing voldoende inzicht kan worden gegeven in gebruikte algoritmen en analysemethoden, met name voor situaties waarin besluitvorming op basis van een Big Data analyse rechtsgevolgen of anderszins een aanmerkelijke impact op burgers heeft. In dit verband zal het kabinet ook onderzoeken of het mogelijk is dat bij ICT-overheidsaanbestedingen kan worden vereist dat de meedingende aanbieders verplicht zijn om de algoritmen die worden ingebouwd in de software voldoende inzichtelijk te maken voor in elk geval de toezichthouder en voor de rechter.
- *Rechtspraak (aanbeveling 1 in § 6.4.5).* Het kabinet zal de Raad voor de Rechtspraak verzoeken zich te oriënteren op de kennis die nodig zal zijn om rechtszaken te kunnen behandelen waarbij Big Data analyses een rol spelen.
- *Autoriteit Persoonsgegevens (aanbeveling 1 in § 6.5).* Het Ministerie van Veiligheid en Justitie en de Autoriteit Persoonsgegevens zijn een traject gestart waarin een onafhankelijk adviesbureau de consequenties in kaart brengt van de versteviging van bevoegdheden en middelen van de Autoriteit door de AVG voor de capaciteit en het budget van dit college.
- *Transparantie (aanbeveling 2 in § 6.5).* Om voor meer transparantie rond Big Data analyses door overheidsdiensten te zorgen, zal het kabinet stimuleren dat deze diensten op hun websites informatie opnemen over het doel van analyses die zij uitvoeren, en de databestanden die daarvoor worden gebruikt.
- *Rechterlijke toetsing (aanbeveling 3 in § 6.5).* Het kabinet zal onderzoeken of uitbreiding van de mogelijkheden voor burgers en belangenorganisaties om zich voor een toetsing van Big Data toepassingen tot de rechter te wenden mogelijk en wenselijk is.
- *Bevorderen van experimenten.* Het kabinet zal binnen de kaders van de huidige en toekomstige wetgeving inzake gegevensbescherming experimenten met Big Data in het veiligheidsdomein starten c.q. voortzetten. Bij deze experimenten zullen de geformuleerde beleidsuitgangspunten leidend zijn en, zo nodig, verder worden uitgewerkt.
- *Implementatie bij rijksoverheid.* Om tot voldoende inbedding van de hiervóór geformuleerde beleidsuitgangspunten binnen de rijksoverheid te komen zal het kabinet ervoor zorgen dat deze worden toegelicht en besproken in in ieder geval het CIO-beraad van het Rijk. De verschillende departementen zullen, via hun CIO's of andere bestaande structuren, er vervolgens voor zorgen dat deze uitgangspunten binnen hun domein in voldoende mate worden verankerd en, voor zover nodig, verder worden uitgewerkt in samenhang met het reguliere beleid, de uitvoering en de handhaving.
- *Implementatie bij andere overheden.* Het kabinet zal in overleg met de VNG en het IPO treden om gezamenlijk te bezien in hoeverre de hiervóór geformuleerde beleidsuitgangspunten ook binnen de andere overheden kunnen worden ingebed.

[18] Raadpleegbaar via www.tweedekamer.nl

- *Dialoog.* Het kabinet zal de dialoog met organisaties die het privacybelang behartigen, over de wijze waarop de overheid de kansen van Big Data wil benutten en over de normen en principes die zij daarbij hanteert, voortzetten en verder versterken.

De eerder geformuleerde beleidsuitgangspunten kunnen in de toekomst eventueel nog worden bijgesteld, voor zover de uitkomsten van de aangekondigde onderzoeken daartoe aanleiding geven.

5. Slot

Het kabinet heeft, zoals eerder gezegd, voor ogen dat er voldoende ruimte moet zijn om de toegevoegde waarde van Big Data verder te verkennen. Dat vergt voldoende vertrouwen in de wijze waarop de risico's die met Big Data gepaard gaan, worden gemitigeerd.

Het kabinet meent met de hiervóór geformuleerde beleidsuitgangspunten en actiepunten een voldoende basis voor dit vertrouwen te leggen. Omdat de ontwikkelingen rond Big Data snel gaan, zal het kabinet in gesprek blijven met partijen die belang bij deze ontwikkelingen hebben, zowel de partijen die ruimte voor Big Data vragen als partijen die voldoende waarborgen rond het gebruik daarvan verlangen. Als daartoe aanleiding bestaat, zal het kabinet uw kamer uiteraard informeren over de verdere ontwikkelingen rond het gebruik van Big Data binnen het veiligheidsdomein en de gesprekken daarover.

De Minister van Veiligheid en Justitie,
G.A. van der Steur