Bijlage

1. Inleiding

In deze bijlage gaat het kabinet meer specifiek op onderdelen van de analyse van de WRR en op de verschillende aanbevelingen uit het rapport in.

2. De ontwikkeling van Big Data in breder perspectief

Het kabinet ziet evenals de WRR in de afgelopen jaren een exponentiële groei van de hoeveelheid data. Deze exponentiële groei zal zich naar verwachting in de komende jaren blijven voortzetten; doordat processorsnelheden, communicatiesnelheden en opslagcapaciteit toenemen, doordat er steeds meer en betere sensoren komen en doordat er steeds meer "dingen" - zoals apparaten, infrastructuur en voertuigen - via internet worden verbonden en gegevens met elkaar kunnen uitwisselen ("internet of things"). Ook technieken om deze grote hoeveelheid informatie te analyseren zijn in ontwikkeling. Grote hoeveelheden data in combinatie met (zelflerende) intelligente algoritmen kunnen leiden tot snellere diagnoses, ondersteunende beslisinformatie of nieuwe inzichten. De beschikbaarheid van data biedt kansen voor integratie en samenwerking van functies. Vraag en aanbod kunnen snel bij elkaar worden gebracht. De deeleconomie is daar een onderdeel van. Data zorgt er bovendien voor dat we kunnen toetsen en scoren, waardoor we veel gemakkelijker kunnen vergelijken welk product, welke dienst of welke persoon het beste is. Producten worden kwalitatief beter en sluiten beter bij onze wensen aan. Burgers kunnen veel meer dan voorheen meedenken, participeren, meebeslissen en kritiek leveren. Big Data maakt het mogelijk om interventies met meer precisie uit te voeren. In de landbouw zijn hier al ontwikkelingen op het terrein van *precision agriculture*, in de geneeskunde maakt gerichte afgifte (*targeted delivery*) de behandeling niet alleen efficiënter, maar worden ook de bijwerkingen geminimaliseerd. Op veiligheidsterrein zien we rond Big Data eenzelfde soort ontwikkeling, waarop hierna in § 4 verder wordt ingegaan.

3. Big Data in het veiligheidsdomein

De WRR beschrijft in § 3 van zijn rapport een zevental cases waarin data-analyses volgens de raad een hoge vlucht hebben genomen. Het kabinet plaatst graag enkele kanttekeningen bij de beschrijving van een van deze cases, het Systeem Risico Indicatie (SyRI), omdat het beeld dat uit deze beschrijving oprijst, naar zijn oordeel enige correctie behoeft.

SyRI is een instrument waarmee gegevensbestanden van gemeenten, UWV, SVB, Inspectie SZW en Belastingdienst kunnen worden gekoppeld ten behoeve van de bestrijding van fraude op het terrein van de sociale zekerheid en de inkomensafhankelijke regelingen, de belasting- en premieheffing en de arbeidswetten. Mede in het licht van de aanbevelingen van de WRR ziet het kabinet SyRI als een goed voorbeeld waarbij niet alleen het verzamelen van gegevens, maar juist ook de wijze waarop gegevens worden geanalyseerd en gebruikt, juridisch is verankerd. Ten behoeve van transparantie en een heldere taak- en verantwoordelijkheidsverdeling is destijds op advies van het College bescherming persoonsgegevens (nu: Autoriteit Persoonsgegevens) een afzonderlijke wettelijke basis voor het instrument gecreëerd. In de Wet SUWI en meer in detail in het Besluit SUWI zijn waarborgen neergelegd met betrekking tot

het gebruik van het instrument. Deze waarborgen betreffen onder meer de voorwaarden waaronder SyRI mag worden ingezet, de soorten gegevens die mogen worden verwerkt, de inperking van de gegevensverzameling, de wijze van gegevensverwerking en de bewaar- en vernietigingstermijnen.[1] Een belangrijke waarborg is ook dat de met behulp van SyRI gegenereerde risicomeldingen niet zomaar mogen worden gebruikt. De betrokken instantie is verplicht te onderzoeken of de desbetreffende persoon of het desbetreffende bedrijf de regels daadwerkelijk heeft overtreden. Pas nadat dit is geconstateerd, kan een sanctie worden opgelegd. Dit spoort met het verbod op geautomatiseerde besluitvorming (zie ook hierna onder 6).

4. Evaluatie van Big data in het veiligheidsdomein

In § 4 van zijn rapport geeft de WRR een evaluatie van Big Data in het veiligheidsdomein. De beperkingen, randvoorwaarden en risico's die de raad met betrekking tot Big Data signaleert, vormen de basis voor zijn aanbevelingen voor een regulatief kader. Op deze aanbevelingen gaat het kabinet hierna in § 6 in.

De WRR noemt in zijn evaluatie een aantal beloftes die Big Data biedt. Ook in de brief waar deze bijlage bij hoort, zijn reeds verschillende beloftes genoemd die Big Data op het terrein van de veiligheid laat zien, waarvan sommige al in enigerlei vorm worden uitgevoerd. Zoals in de brief is vermeld, worden die beloftes in deze bijlage nog wat verder uitgewerkt en aangevuld, met de kanttekening dat verschillende beloftes (nog) maar ten dele de kenmerken van Big Data vertonen.

Hansken
Met de voortschrijdende digitalisering van de samenleving en de criminaliteit groeit de hoeveelheid data op gegevensdragers die in strafzaken in beslag wordt genomen. Binnen de politie wordt de forensische zoekmachine Hansken gebruikt om grote hoeveelheden gegevens afkomstig van in beslaggenomen gegevensdragers (zoals telefoons, computers, laptops, harde schijven en dergelijke) te kunnen onderzoeken en te ordenen. Deze zoekmachine kan worden ingezet om gegevensdragers door te spitten op relevante gegevens en deze geordend weer te geven. De snelheid waarmee dat gepaard gaat, is zeer belangrijk voor de scenariovorming rond een strafzaak, het in beeld brengen van slachtoffers en het rond krijgen van het digitaal bewijs. Zo kan in een kinderpornozaak tijd het verschil maken in het kunnen ontzetten van een slachtoffer uit een acute misbruiksituatie.

Raffinaderij-concept
De politie wordt in het opsporingsproces steeds vaker geconfronteerd met grote hoeveelheden gestructureerde en ongestructureerde data waaruit nuttige informatie kan worden verkregen, als er hulpmiddelen beschikbaar zijn die de medewerkers in staat stellen op een effectieve en efficiënte manier daadwerkelijk gebruik te maken van al die data. Het Raffinaderij-concept is een pilot binnen de politie om hier ervaring mee op te doen. Het is een voorziening die het mogelijk maakt om snel grote hoeveelheden politiegegevens te ontsluiten, betekenis te geven, in samenhang met elkaar te analyseren en visualiseren. Daarmee kunnen bijvoorbeeld, gemakkelijker dan met de traditionele voorzieningen mogelijk is, relaties tussen gebeurtenissen en/of personen zichtbaar worden gemaakt of juist in een vroeg stadium worden ontkracht. Zo worden relaties zichtbaar tussen

[1] Zie ook: Kamerstukken II 2014/15, 17050, 489.

gebeurtenissen die met een traditionele aanpak niet zo snel met elkaar in verband gebracht konden worden. Dat maakt proactieve en effectieve aanpak van criminaliteit mogelijk. Op een beperkt aantal landelijke thema's (liquidatieonderzoeken en contraterrorisme) wordt er binnen de opsporing mee gewerkt.

Signaleringstool Integrale Handhaving
Almere, Tilburg en Eindhoven hebben afzonderlijk een signaleringstool ontwikkeld. De tools koppelen interne systemen zodat heel eenvoudig zichtbaar wordt dat er handhavingsacties op een bepaald adres lopen en vanuit welke onderdelen van de gemeentelijke organisatie die lopen. Hierdoor kan effectiever en efficiënter worden gehandhaafd. Breda en Nijmegen zijn geïnteresseerd om deel te nemen en de drie gemeenten zijn net gestart met werving van andere gemeenten.

Datamodel en tool koppeling basisregistraties[2]
Het idee achter dit model is om relevante gegevens uit de (gemeentelijke) basisregistraties en kernregistraties in samenhang te ontsluiten en visualiseren met behulp van een analysetool die krachtige rekenregels bevat. Daarmee kunnen complexe analyses en (gemeente overstijgende) netwerken inzichtelijk worden gemaakt voor toepassing op beleid en uitvoering op het terrein van de veiligheid. Breda is de trekker. Eindhoven, Tilburg en Almere zijn geïnteresseerd om deel te nemen.

Risico-analyse door inspecties
De Inspectie Sociale Zaken en Werkgelegenheid (ISZW) bepaalt door de analyse van gegevens uit diverse bronnen waar de risico's het grootst zijn. Dit biedt inspecteurs van ISZW, naast hun ervaring en deskundigheid, goed onderbouwde informatie om gerichter hun werk te doen. De dataverzameling gebeurt per project, met inachtneming van de wettelijke grondslagen en de principes van dataminimalisatie en doelbinding.

"Dynamische monitoren" bij de Belastingdienst
De Belastingdienst bouwt met "Dynamisch Monitoren" een actueel en integraal klantbeeld van mensen op die een belastingschuld hebben openstaan. "Dynamisch Monitoren" koppelt openstaande vorderingen aan bronnen voor verhaalsmogelijkheden (loon, auto, vastgoed etc.) en genereert op basis daarvan een lijst van vorderingen met (nieuwe) verhaalsmogelijkheden. Voorheen moest een incasso-medewerker allerlei systemen en schermen openen om een integraal beeld van een belastingschuldige op te bouwen. Dit is erg inefficiënt en foutgevoelig en biedt bovendien geen structurele manier om continu en automatisch op nieuwe, actuele verhaalsmogelijkheden te toetsen. Daarnaast is de medewerker in staat om maatwerk te leveren, omdat hij inzicht heeft in het gedrag en de persoonlijke situatie van de belastingschuldige. Dit kan de effectiviteit van de interventies verhogen en bijdragen tot verbetering van de naleving van de belastingwetgeving, omdat de burger zich beter behandeld voelt.

FinPro
Binnen het project FinPro zijn in de afgelopen twee jaar in Rotterdam twee wetenschappelijke onderzoeken uitgevoerd naar de mogelijkheden van het

[2] Dit en het vorige voorbeeld komen uit de gemeentelijke praktijk. Zie voor meer voorbeelden van data-innovatie bij gemeenten, ook op andere terreinen dan veiligheid: http://magazine.kinggemeenten.nl/data-en-gemeenten/#!/inhoud.

combineren van data uit zeer diverse bronnen voor het inzichtelijk maken van fraude en ondermijnende criminaliteit. Het project had niet tot doel om strafbare feiten op te sporen en vervolgens tot vervolging over te gaan, maar enkel om tot dan toe onbekende fraudepatronen in beeld te brengen.[3]

Controle van dijken
Om de veiligheid van dijken te monitoren kunnen burgers worden ingezet (*crowd sourcing*) die via hun smart phone foto's opsturen waarop (mogelijke) gebreken aan een dijk zichtbaar worden gemaakt. Efficiënter dijkbeheer en kostenreductie zijn het positieve effect. Waterschappen experimenteren hiervoor reeds met proefprojecten. Een Big Data aanpak is nodig omdat er een koppeling van data van verschillende aard en uit verschillende bronnen moet plaatsvinden en inpasbaar gemaakt in een betrouwbaar monitoringsysteem.

Landelijk Meetnet Luchtkwaliteit
Er liggen veel kansen bij het gebruik van sensortechnologie en het Internet of Things. Burgers kunnen met goedkope sensoren bijdragen aan het Landelijk Meetnet Luchtkwaliteit. De eerste verkenningen zijn gestart en een prototype is inmiddels ontwikkeld. Een positieve ontwikkeling voor burgers met aandoeningen aan de luchtwegen door adviezen op maat over de lokale luchtkwaliteit ligt in het verschiet.

Verbetering verkeersveiligheid
Door koppeling van data met betrekking tot het weer aan data over verkeersstromen kan de doorstroming op de weg verbeteren. Dit komt ten goede aan de verkeersveiligheid en betere bereikbaarheid van belangrijke economische knooppunten in Nederland.

5. Big Data, veiligheid en de juridische kaders voor gegevensverwerking

Het kabinet kan zich in het algemeen goed vinden in de beschrijving van de juridische kaders voor het uitvoeren van Big Data analyses die de WRR in zijn rapport heeft opgenomen. Deze kaders vallen voor een belangrijk deel samen met de volgende acht toetsstenen die het kabinet in een brief van 20 mei 2015 aan de Tweede Kamer in zijn visie op privacybescherming naar voren heeft gebracht:

1. Is de verwerking van persoonsgegevens noodzakelijk voor een legitiem doel?
2. Voldoet de verwerking van persoonsgegevens aan de eisen van proportionaliteit en subsidiariteit?
3. Is de doelbinding wettelijk vastgelegd en voldoende ingekaderd?
4. Is er een adequate regeling van toegang tot de persoonsgegevens?
5. Zijn de persoonsgegevens goed beveiligd?
6. Zijn de bewaartermijnen goed geregeld?
7. Is er, waar nodig, een Privacy Impact Assessment (PIA) uitgevoerd?
8. Is het toezicht op de verwerking van persoonsgegevens goed geregeld?[4]

---

[3] Zie Kamerstukken II 2015/16, Aanhangsel 3413.

[4] Kamerstukken II 2014/15, 32 761, nr. 83, blz. 2. Ook de Privacycoalitie heeft gewezen op het belang van het noodzakelijkheidsvereiste en het vereiste van doelbinding bij data-analyses. Deze vereisten, die in de AVG zijn vastgelegd, impliceren dat er altijd een valide redenering moet zijn om bepaalde datasets in een Big Data analyse te betrekken en dat niet lukraak bestanden aan elkaar gekoppeld mogen worden.

De beschrijving van de juridische kaders door de WRR nodigt evenwel op sommige punten ook uit tot het maken van een kanttekening.

De WRR stelt zich in § 5.3.1 op het standpunt dat, wanneer de politie gegevens op rechtmatige wijze heeft verzameld, er vervolgens minder zwaar toezicht op het hergebruik van deze gegevens is, bijvoorbeeld in het kader van een ander strafrechtelijk onderzoek. De Raad verbindt daaraan de conclusie dat binnen de juridische kaders voor gegevensverwerking door politie en justitie dus gedeeltelijk een hiaat ten aanzien van de uitvoering van Big Data analyses bestaat. Het kabinet wijst er evenwel op dat het hergebruik van gegevens die met de inzet van bepaalde bijzondere opsporingsbevoegdheden, zoals observatie met behulp van een technisch hulpmiddel, zijn verzameld, in het kader van een ander strafrechtelijk onderzoek ingevolge de artikelen 126cc en 126dd WvSv weliswaar mogelijk is, maar ook aan grenzen is gebonden. Denk daarbij aan het vereiste dat een officier van justitie daarvoor toestemming moet geven. Verder is verwerking van gegevens door politie en justitie bij Big Data analyses volledig aan toezicht door de Autoriteit Persoonsgegevens onderworpen. Er bestaat op dat punt dan ook geen verschil met de fase waarin gegevens worden verzameld.

In § 5.4.1 stelt de WRR zich op het standpunt dat het verder verwerken van gegevens alleen mag plaatsvinden in het kader van een wettelijk omschreven taak of bevoegdheid en dat uit het verbod op verdere verwerking voor andere doeleinden volgt dat secundair gebruik in principe niet is toegestaan. Hoewel de WRR er ook op wijst dat de doelen van organisaties op het veiligheidsterrein vaak ruim zijn omschreven en daardoor de doelbinding een zekere rekkelijkheid geven, meent het kabinet dat de WRR hier een te beperkte uitleg aan het principe van doelbinding geeft. Dit principe laat verdere verwerking voor andere doeleinden toe, mits deze niet onverenigbaar zijn met de doeleinden waarvoor de gegevens oorspronkelijk zijn verzameld (vgl. artt. 9, eerste en tweede lid, Wet bescherming persoonsgegevens (Wbp) en art. 5, eerste lid, onder b, en 6, vierde lid, AVG). Wel moet uiteraard rekening worden gehouden met eventuele geheimhoudingsplichten.

In diezelfde paragraaf wijst de WRR erop dat het combineren van publieke gegevens met private data steeds vaker voorkomt en stelt de Raad dat overheidsorganisaties zich daarmee steeds meer op terreinen begeven die niet traditioneel tot hun takenpakket behoren. Het kabinet vraagt zich evenwel af of deze conclusie juist is. Ook de verwerking van private data kan immers een publiek belang dienen dat wel degelijk binnen de reikwijdte van het takenpakket van die organisaties valt. Zo kunnen gegevens van een bank die op fraude duiden, van groot belang zijn voor samenwerkingsverbanden die fraudebestrijding als doel hebben.

Verder valt op dat de WRR zich in § 5.4.1 op het standpunt stelt dat in het domein van veiligheid steeds vaker ook de gegevens van "niet-verdachte personen" verzameld en verwerkt worden in onderzoeken, controle, toezicht en recherchewerk, hetgeen op gespannen voet zou staan met de onschuldpresumptie. Het kabinet beaamt dat voor het verzamelen en verwerken van gegevens van onverdachte burgers gegronde redenen moeten bestaan en dat met dit type gegevens in een Big Data analyse gelet op de mogelijke gevolgen extra zorgvuldig moet worden omgegaan, maar ziet niet goed waarom dit op gespannen voet met de onschuldpresumptie zou staan. De uitkomst van de analyse kan leiden tot bijvoorbeeld een lijst waarop personen staan met kenmerken die op een verhoogd risico wijzen dat zij beroepsfraudeur zijn, maar

die nog geen verdachte zijn. Omdat er sprake is van correlatie en niet van causaliteit, kan immers van een formele verdenking (nog) geen sprake zijn. Daarvoor dienen concrete feiten en omstandigheden met betrekking tot de desbetreffende persoon op tafel te komen die op fraude wijzen. Om te garanderen dat de verdenking op dit punt deugdelijk is, is bij de toepassing van strafvorderlijke bevoegdheden menselijke tussenkomst nodig.[5] De onschuldpresumptie is dan ook een strafvorderlijk beginsel dat personen, zolang het tegendeel niet is bewezen, voor onschuldig houdt, maar is geen beginsel dat aan het recht op bescherming van persoonsgegevens ten grondslag ligt. Daarvoor gelden andere waarborgen, zoals de grondslagen voor rechtmatige gegevensverwerking die in artikel 8 Wbp en artikel 6 AVG zijn vastgelegd, en geldt de bescherming van bijzondere persoonsgegevens, zoals neergelegd in de artikelen 16 e.v. Wbp en artikel 9 AVG.

De WRR constateert in § 5.4.2 terecht dat er spanning kan bestaan tussen principes van gegevensbescherming en het verzamelen van gegevens voor Big Data analyses. Het gaat dan vooral om het noodzakelijkheidsvereiste en het principe van doelbinding. Deze spanning wordt veroorzaakt doordat er enerzijds een duidelijk, specifiek doel moet zijn voor het verzamelen van gegevens, maar anderzijds het doel en de noodzaak van de verwerking vaak pas duidelijk worden na het combineren van de gegevens met elkaar of met andere gegevens. Dat is de kern van Big Data. Uiteraard moet er voor het verzamelen van persoonsgegevens een wettelijke grond bestaan. Dit geldt voor alle persoonsgegevens die verzameld worden, of dit nu gegevens uit open bronnen zijn, gegevens die voortkomen uit de uitoefening van bijzondere bevoegdheden dan wel gegevens die afkomstig zijn van derden. Tegelijkertijd is het kabinet met de WRR van oordeel dat in relatie tot Big Data analyses primair behoefte is aan het versterken van de waarborgen in de fase nà het verzamelen, waarvoor thans al stevige waarborgen gelden. Deze kabinetsreactie ziet aldus op versterking van de waarborgen in de fase van het analyseren en de besluitvorming op basis van de uitkomsten daarvan. Om het potentieel van Big Data te kunnen benutten is het immers noodzakelijk dat rechtmatig verzamelde gegevens beschikbaar zijn en blijven, en (her)gebruikt kunnen worden voor analyses.

Aan het slot van § 5.6.2 stelt de WRR zich op het standpunt dat het steeds onduidelijker wordt welk regime van toepassing is op data-analyses in samenwerkingsverbanden en de daaruit verkregen informatieproducten en kennis. Het kabinet wil dit standpunt in zoverre nuanceren dat samenwerkingsverbanden data-analyses mogen uitvoeren om bepaalde patronen zichtbaar te maken. Zij kunnen daartoe gebruik maken van de mogelijkheden in de huidige (en toekomstige) wetgeving om ten behoeve van wetenschappelijk onderzoek en statistiek persoonsgegevens te verwerken.[6] Het kabinet wijst ook op de waarborgen die de huidige wettelijke kaders en in de toekomst de AVG en de Richtlijn bevatten met betrekking tot het uitvoeren van data-analyses.[7] Niettemin ligt in de huidige praktijk van data-analyse binnen samenwerkingsverbanden een belangrijke aanleiding voor het kabinet om een wetsvoorstel voor te bereiden voor een Kaderwet gegevensuitwisseling in

---

[5] Op het aspect van menselijke tussenkomst wordt hierna in § 6 nader ingegaan.

[6] Zie artikel 9, derde lid, en 23, tweede lid, Wet bescherming persoonsgegevens, artikel 22 Wet politiegegevens en de artikelen 15 en 39g Wet justitiële en strafvorderlijke gegevens, alsmede artikel 5, eerste lid, onder b en e, 9, tweede lid, onder j, en 89, eerste en tweede lid, van de AVG en artikel 4, derde lid, en 9, tweede lid, van de Richtlijn.

[7] Zie de waarborgen die hierna in § 6 worden genoemd.

samenwerkingsverbanden.[8] Het kabinet meent evenwel dat dit vraagstuk zich in een bredere context voordoet dan alleen samenwerkingsverbanden. Het wil dan ook 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.

6. Conclusies en aanbevelingen

In § 6.4 en 6.5 formuleert de WRR een aantal aanbevelingen met betrekking tot de invulling van het door de Raad voorgestelde regulatieve kader voor Big Data, respectievelijk het toezicht op de verwerking van Big Data, de transparantie van die verwerking en de uitoefening van rechterlijke toetsing. Het kabinet geeft hierna per aanbeveling zijn reactie daarop.

Aanbeveling 1 in § 6.4.1: Gebruik Big Data in de eerste plaats voor de analyse van veiligheidsvraagstukken die zich goed voor patroonherkenning lenen en waarover data met een hoog onderscheidend vermogen beschikbaar zijn.

De WRR verbindt hieraan in § 6.3 de conclusie dat datamining als voor Big Data kenmerkende analysevorm voor het voorkomen van terroristische aanslagen waarschijnlijk een ineffectieve methode is. In de internationale strijd tegen het terrorisme speelt een snelle analyse van grote hoeveelheden data evenwel een doorslaggevende rol. Zo wordt binnen het Europees platform van de Counter Terrorism Group dat recent is opgericht met als doel de bestrijding van cellen van ISIS in Europa, veelvuldig *realtime* data uitgewisseld. Door grote hoeveelheden (ruwe) data inzake communicatie met elkaar te combineren, kunnen netwerken en contacten worden blootgelegd die anders verborgen blijven. Dit heeft geleid tot een aantal arrestaties van mogelijke *operatives* van ISIS in Europa. Zonder de beschikbaarheid van de (big) data waren deze arrestaties niet of mogelijk niet tijdig verricht.

De aanbeveling van de WRR dat gebruik van Big Data voor de analyse van veiligheidsvraagstukken in de eerste plaats geschikt is bij vraagstukken met een regelmatig en terugkerend karakter die zich daardoor goed voor patroonherkenning lenen, kan als uitgangspunt niettemin worden onderschreven. 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. Dat neemt niet weg dat waakzaamheid bij toepassing van Big Data analyse bij dergelijke vraagstukken geboden blijft, zeker naarmate de potentiële impact daarvan op individuele burgers groter is.

Aanbeveling 2 in § 6.4.1: Zorg bij de inzet van Big Data voor een evenwichtige spreiding van doeleinden. Gebruik Big Data behalve voor repressieve doeleinden ook voor dienstverlening gericht op preventie, die rechtstreeks ten goede komt aan burgers, private organisaties en bedrijven.

Het kabinet is een voorstander van het actief ontsluiten van open data om het overheidshandelen transparanter te maken en mogelijk maatschappelijke meerwaarde te creëren.[9] Het kabinet onderschrijft dat de uitkomsten van Big Data analyses in beginsel ook kunnen worden gedeeld met buurtcomités en

[8] Zie Kamerstukken II 2014/15, 32761, nr. 79, blz. 9.

[9] Kamerstukken II 2015/16, 32802, nr. 20.

bedrijven in het kader van preventie. Wel zal dit met meer waarborgen moeten worden omkleed dan het beschikbaar stellen van louter ruwe data. Steeds zal per geval moeten worden beoordeeld of openbaarmaking van de uitkomst van de analyse bijdraagt aan het gewenste effect (preventie) en zal daaraan voorafgaand een zorgvuldige risicoanalyse moeten plaatsvinden. Dat geldt zeker voor gevallen waarin de analyses een voorspellend karakter hebben. Het kabinet wijst in dit verband op het Criminaliteit Anticipatie Systeem (CAS), waaraan ook in het rapport van de WRR uitgebreid aandacht wordt besteed. De twee voornaamste doelstellingen van CAS zijn criminaliteitspreventie en optimalisatie van politie-inzet. Het openbaar maken van de resultaten van deze analyses zou een aanvulling kunnen vormen op de bestaande dienstverlening, waarbij de politie via de website politie.nl (pogingen tot) woninginbraken laat zien op postcodegebied. Het kabinet tekent hierbij echter aan dat er verkeerde gevolgtrekkingen kunnen worden gemaakt of ongewenste effecten kunnen optreden bij het openbaar maken van de resultaten. Om die reden zou op grond van een risico-afweging ook kunnen worden besloten om niet direct die resultaten zelf openbaar te maken, maar in plaats daarvan op basis van die resultatenanalyse in overleg met burgers en bedrijfsleven preventieve maatregelen te treffen.

Aanbeveling 1 in § 6.4.4: Gegeven de ruimere bevoegdheden van overheidsorganisaties op het terrein van misdaad- en fraudebestrijding en gegeven de toename in de omvang van gegevensverwerkingsprocessen moeten zij een wettelijk te omschrijven zorgplicht voor de analyse van gegevens in acht nemen.
Het is onwerkbaar om vooraf exact voor te schrijven waaraan de analysefase moet voldoen: dat is per geval verschillend. Wel geldt een aantal algemene vereisten voor de kwaliteit van de data en de deugdelijkheid van de gehanteerde analysemethoden:

1. *Overheidsdiensten moeten ervoor zorgen dat hun gegevens up to date zijn en dat hun datasets geen bias bevatten, een plicht die zich tevens uitstrekt tot gegevens die zij van derden verkrijgen.*
2. *De algoritmen en methoden die bij data-analyses worden gebruikt moeten deugdelijk zijn en aan de wetenschappelijke criteria voor goed (statistisch) onderzoek voldoen.*
3. *Ze moeten daarom voor toezicht toegankelijk zijn, wat problematisch kan zijn als het 'hart' van analysesystemen uit commerciële algoritmen bestaat, die de datadienstverleners als bedrijfsgeheim presenteren. Hierbij moeten de onderzoeksresultaten, de profielen en correlaties ook op hun merites worden gecontroleerd: de gegevensverwerkende partijen moeten duidelijk kunnen maken hoe zij tot bepaalde uitkomsten komen.*

Overheidsdiensten zien ook buiten de toepassing van Big Data analyses de noodzaak tot het goed *up to date* houden van hun gegevens. Deze gegevens zijn immers vaak gekoppeld aan hun primaire taakuitvoering. Iedere gegevensbron zal in mindere of meerdere mate een *bias* (afwijking) bevatten. Daarom is het van groot belang daarmee in de analyse- en gebruiksfase rekening te houden. In de meeste gevallen kan een bias worden gedetecteerd door middel van statistische analyse en kunnen mitigerende maatregelen getroffen worden om alsnog een zinvolle en objectieve analyse te kunnen plegen. Denk hierbij aan onder meer het betrekken van domeinexperts om goed te kunnen begrijpen welke bias aanwezig zou kunnen zijn.

Een zorgplicht voor overheidsdiensten om ervoor te zorgen dat hun gegevens up to date zijn en een zo gering mogelijke bias bevatten, vloeit nu al voort uit artikel

11, tweede lid, Wbp. Daarin is vastgelegd dat degene die persoonsgegevens verwerkt, de nodige maatregelen moet treffen om ervoor te zorgen dat deze gegevens juist en nauwkeurig zijn. Het gaat hier om een inspanningsverplichting. Een garantie voor de juistheid van gegevens kan van degene die de analyse uitvoert, niet worden gevergd. Wel dient hij alle maatregelen te treffen die in redelijkheid van hem kunnen worden gevraagd. De redelijkheid stelt daarbij, afhankelijk van bij voorbeeld de soort gegevens die onderwerp van verwerking zijn, de stand van techniek en de kosten die met de maatregelen gepaard gaan, grenzen aan de te nemen maatregelen.[10] Een dergelijke zorgplicht vloeit ook voort uit artikel 5, eerste lid, onder d, van de AVG, waarin is bepaald dat persoonsgegevens juist moeten zijn en zo nodig moeten worden geactualiseerd, waarbij alle redelijke maatregelen moeten worden genomen om de persoonsgegevens die, gelet op de doeleinden waarvoor zij worden verwerkt onjuist zijn, onverwijld te wissen of te rectificeren. In artikel 4, eerste lid, onder d, van de Richtlijn gegevensbescherming opsporing en vervolging is een hiermee vergelijkbare bepaling opgenomen. Daarnaast kan uitoefening van het in artikel 16 van de AVG en de Richtlijn vastgelegde correctierecht bijdragen aan de juistheid van gebruikte persoonsgegevens.

Het kabinet is het ook eens met de opvatting van de WRR dat algoritmen en methoden die bij data-analyses worden gebruikt deugdelijk moeten zijn en aan de wetenschappelijke criteria voor goed (statistisch) onderzoek moeten voldoen. Bij voorkeur worden algoritmen gebruikt die wetenschappelijk zijn getoetst, blijkend uit bijvoorbeeld publicaties of peer reviews. Veelgebruikte algoritmen zijn doorgaans dan ook wetenschappelijk gevalideerd. In meer algemene zin is het van groot belang dat er, zoals dat bij ieder (software)ontwikkeltraject het geval is, voldoende aandacht is voor de kwaliteit van het zowel het proces alsook het valideren van de resultaten. Een zorgplicht met betrekking tot de deugdelijkheid van gebruikte algoritmen en methoden ligt opgesloten in artikel 5, eerste lid, onder a, van de AVG, waarin is bepaald dat persoonsgegevens moeten worden verwerkt op een wijze die ten aanzien van de betrokkenen behoorlijk is. Een hiermee vergelijkbare bepaling is terug te vinden in artikel 4, eerste lid, onder a, van de Richtlijn, waarin wordt gesproken over de noodzaak van "eerlijke" verwerking. Het is voor het kabinet evident dat onder "behoorlijke" c.q. "eerlijke" verwerking ook een gebruik van deugdelijke algoritmen valt.

De WRR huldigt naar het oordeel van het kabinet terecht de opvatting dat gebruikte algoritmen voor toezicht en rechterlijke toetsing inzichtelijk dienen te zijn. Dat is nodig in het geval dat een toezichthouder of rechter een oordeel moet geven over de toelaatbaarheid van een bepaalde vorm van Big Data analyse. Dit impliceert dat, zoals ook de Privacycoalitie aanbeveelt, de nadruk zou moeten liggen op verklaarbare voorspellingen. Het kabinet bestudeert nog hoe hieraan het best invulling kan worden gegeven. Het wil daarbij onderzoeken of, indien de besluitvorming op basis van een Big Data analyse rechtsgevolgen of anderszins een aanmerkelijke impact op burgers heeft, uitgangspunt dient te zijn dat de logica achter de analyse en dus de gebruikte algoritmen transparant zijn. Daarbij zal ook aandacht worden besteed aan de vraag of het nuttig en mogelijk is om bij de aanbesteding van de bouw van een systeem waarbinnen voorgenomen Big Data verwerkingen zullen plaatsvinden, als voorwaarde te stellen dat de algoritmen die worden ingebouwd in de software voldoende inzichtelijk zijn voor in elk geval de toezichthouder en voor de rechter.

[10] Kamerstukken II 1997/98, 25892, nr. 3, blz. 97.

Aanbeveling 2 in § 6.4.4: Big Data projecten en –toepassingen in het veiligheidsdomein moeten onderwerp zijn van een externe review door de toezichthouder, die in het bijzonder toeziet op de gemaakte keuzes inzake data en methode van analyse. Deze review toetst ook of er aan de zorgplicht is voldaan.

Het kabinet onderschrijft het belang van het uitvoeren van *reviews*, waaronder wij begrijpen het toetsen van de gemaakte keuzes inzake data en methode van analyse aan algemene juridische en kwaliteitseisen. Wel vraagt het zich af of àlle Big Data projecten en -toepassingen in het veiligheidsdomein onderwerp van een externe toetsing dienen te zijn. Het kabinet meent die vraag ontkennend te moeten beantwoorden, omdat het naar zijn oordeel meer voor de hand ligt om aan te sluiten bij de regeling van gegevensbeschermingseffectbeoordelingen in de AVG en de Richtlijn. In de AVG is bepaald dat de verwerkingsverantwoordelijke een gegevensbeschermingseffectbeoordeling uitvoert wanneer een soort verwerking, in het bijzonder een verwerking waarbij nieuwe technologieën worden gebruikt, gelet op de aard, de omvang, de context en de doeleinden daarvan waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen (artikel 35, eerste lid). Artikel 35, derde lid, onder a, AVG vereist meer in het bijzonder een gegevensbeschermingseffectbeoordeling wanneer sprake is van een systematische en uitgebreide beoordeling van persoonlijke aspecten, die is gebaseerd op geautomatiseerde verwerking, waaronder profilering, en waarop besluiten worden gebaseerd waaraan voor de natuurlijke persoon rechtsgevolgen zijn verbonden of die de natuurlijke persoon op vergelijkbare wijze treffen. Het zal van de aard van de desbetreffende Big Data analyse afhangen of deze in het licht van voornoemde bepalingen vooraf moet worden gegaan door een gegevensbeschermingseffectbeoordeling. Als een gegegevensbeschermingseffectbeoordeling dient plaats te vinden, ligt het voor de hand daarin ook een verantwoording van de gemaakte keuzes inzake data en methode van analyse, zoals bedoeld in het WRR-rapport, op te nemen. Bij de komende aanpassing van het huidige toetsmodel Privacy Impact Assessment Rijksdienst, dat onlangs is geëvalueerd[11], zal worden bezien op welke wijze deze elementen van Big Data verwerkingen een plaats kunnen krijgen in het toetsmodel. Dit model geldt voor voorgenomen verwerkingen op alle beleidsdomeinen, waaronder het veiligheidsdomein.

De AVG schrijft ook voor dat, indien nodig, de verwerkingsverantwoordelijke toetst of de verwerking overeenkomstig deze beoordeling wordt uitgevoerd, zulks ten minste wanneer sprake is van een verandering van het risico dat de verwerkingen inhouden (artikel 35, elfde lid). Een hiermee vergelijkbare bepaling ontbreekt in de Richtlijn.[12] Bij de implementatie van de Richtlijn zal worden bezien of een dergelijke bepaling niettemin in de implementatiewetgeving dient te worden opgenomen. Wanneer uit een gegevensbeschermingseffectbeoordeling blijkt dat de verwerking een hoog risico zou opleveren indien de verwerkingsverantwoordelijke geen maatregelen neemt om het risico te beperken, dient hij de toezichthoudende autoriteit te raadplegen alvorens tot verwerking mag worden overgegaan (artikel 36 AVG en artikel 28 Richtlijn). Deze werkwijze waarborgt op passende wijze de mogelijkheid tot het uitoefenen van extern toezicht door de Autoriteit Persoonsgegevens en de functionaris voor gegevensbescherming.

---

[11] Zie Kamerstukken I 2015/16, 31051, nr. H.

[12] Wel bevat de Wet politiegegevens in artikel 33 bepalingen over het houden van privacy audits.

Aanbeveling 3 in § 6.4.4: 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

De WRR heeft hierbij voor ogen dat het desbetreffende project binnen het gegeven tijdsbestek wordt geëvalueerd, waarbij wordt nagegaan of de noodzaak voor het project nog steeds bestaat, het gegevensverwerkingsproces effectief was en een kosten-batenanalyse wordt gemaakt. De raad adviseert hiervoor aan te sluiten bij de zgn. Surveillance Impact Assessments, die meeromvattend zijn dan een Privacy Impact Assessment. De evaluatie zal moeten uitmonden in een rapport dat naar de toezichthouder wordt gestuurd.

Big Data projecten lenen zich bij uitstek voor een aanpak waarbij stap voor stap en multidisciplinair wordt gewerkt. Deze aanpak impliceert dat doorlopend evaluaties van de behaalde resultaten plaatsvinden. Bij deze evaluaties zullen de behaalde resultaten nadrukkelijk moeten worden afgewogen tegen het belang van bescherming van persoonsgegevens. Een projectstructuur waarbij pas na een aantal (van 3 tot 5) jaar functionaliteit wordt opgeleverd, past minder goed bij die methodiek. Vanwege het inrichten van een data infrastructuur, een data architectuur en het op sterkte krijgen van de benodigde Big Data expertise zullen grote dataverwerkingsprojecten echter wel een doorlooptijd van één tot enkele jaren nodig kunnen hebben.

Met betrekking tot de suggestie van het uitvoeren van zgn. Surveillance Impact Assessments is het kabinet van oordeel dat het uitvoeren van een gegevensbeschermingseffectbeoordeling, zoals geregeld in de AVG en de Richtlijn, afdoende is.

Het uitbreiden van de taak van de Autoriteit Persoonsgegevens met toezicht op de doelmatigheid en effectiviteit van ICT toepassingen in het algemeen of Big Data toepassingen in het bijzonder is niet wenselijk. Deskundigheid bij de Autoriteit Persoonsgegevens op dit terrein bestaat momenteel niet, aangezien toezicht daarop niet tot hun taakgebied behoort. Daar komt bij dat er reeds andere instanties bestaan, zoals de Algemene Rekenkamer, voor wie dit aspect wel tot de kerntaken behoort en die daarvoor de benodigde expertise heeft. De afweging of de noodzaak van een project nog bestaat en de doelen wel, niet of gedeeltelijk zijn behaald is daarbij een taak van de desbetreffende projectstuurgroep c.q. opdrachtgever.

Aanbeveling 1 in § 6.4.5: De WRR beveelt aan om bij profiling nadere regels over toelaatbare foutmarges te stellen, het verbod op geautomatiseerde besluitvorming strikter te handhaven en alert te zijn op semi-automatische besluitvorming.

Toelaatbare foutmarges
Bij het gebruik van Big Data analysetechnieken die uitmonden in profielen, spelen foutmarges een belangrijke rol. Ze geven aan hoe goed het voorspellend vermogen van een profiel is. Toepassing van profielen op concrete situaties levert vrijwel altijd een foutmarge op, omdat een profiel altijd over- of onderinclusief is. Afhankelijk van de impact op privacy en veiligheid en de zeldzaamheid van het fenomeen wordt bepaald welke foutmarge toelaatbaar is. Wanneer de gevolgen van het gebruik van de profielen voor het individu of de maatschappij groter worden, neemt ook het belang van adequate *benchmarks* toe.

Toelaatbare foutmarges bij profiling worden door de specifieke context van de desbetreffende analyse bepaald. Het is daarom wenselijk die door de betrokken organisaties zelf te laten opstellen en deze vervolgens 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.

Het verbod op geautomatiseerde besluitvorming
Voor de toepassing van het WRR-rapport en deze kabinetsreactie daarop, is het van belang om vast te stellen dat het hier gaat om geautomatiseerde besluitvorming met gebruikmaking van Big Data analyses, inclusief profiling. Geautomatiseerde besluitvorming kan vanzelfsprekend ook plaatsvinden zonder Big Data analyses[13], maar dat valt buiten de reikwijdte van deze brief.

Het verbod op geautomatiseerde besluitvorming waar de WRR op doelt, is het verbod dat in artikel 42 van de Wet bescherming persoonsgegevens is opgenomen. Dat verbod gaat over situaties waarin sprake is van een besluit waaraan rechtsgevolgen zijn verbonden of dat betrokkene in aanzienlijke mate treft, terwijl dat besluit alleen wordt genomen op grond van een profiel dat is opgesteld op basis van geautomatiseerde verwerking van persoonsgegevens, waarbij het profiel ertoe dient een beeld te krijgen van bepaalde, typische kenmerken van de desbetreffende personen. Gelet op het risico van fouten en ondeugdelijke interpretaties onderschrijft het kabinet de noodzaak om dat verbod te handhaven, omdat er anders een onnodige kans op discriminatie en stigmatisering bestaat. Soortgelijke bepalingen staan opgenomen in de AVG en de Richtlijn gegevensbescherming opsporing en vervolging (artikel 22, eerste lid, resp. 11, eerste lid). Op grond van beide regelingen zijn er uitzonderingen mogelijk op het verbod, mits voorzien is in passende waarborgen voor de rechten en vrijheden van betrokkene.

Big Data en menselijke tussenkomst
Er zijn uiteenlopende situaties denkbaar die formeel niet onder de genoemde verbodsbepalingen vallen, maar waarbij materieel wel sprake is van Big Data analyses die tot gevolgen (kunnen) leiden voor individuen of groepen. Dit onderdeel gaat over dergelijke situaties. Ondanks het feit dat het verbod voor die situaties niet geldt, is er aanleiding om te bezien welke risico's er bestaan rondom die vormen van gegevensverwerking, en te kijken naar de mate van menselijke tussenkomst die gewenst is.

In de praktijk gaat het om situaties waarin sprake is van semi-automatische besluitvorming. Dit is de situatie waarin wel sprake kan zijn van een besluit met rechtsgevolg of aanmerkelijk gevolg, maar waarbij de computer-analyse door een menselijke beslisser wordt gevolgd zonder enige nadere oordeelsvorming. Het betreft dan het bekende (en frustrerende) "Computer says no".

Met het oog op de hiervóór genoemde risico's die het verbod op geautomatiseerde besluitvorming kan mitigeren (voorkomen van fouten, discriminatie en stigmatisering) is van belang dat de menselijke inbreng iets moet toevoegen aan of een betekenisvol oordeel moet vellen over de uitkomst van de analyse zelf.

[13] Een voorbeeld hiervan is het volledig geautomatiseerde proces van het opleggen van een snelheidsboete.

Indien de analyse een bepaalde beslissing indiceert, dient de analyse te worden getoetst op fouten en ondeugdelijke interpretaties en de beslissing aan een menselijke noodzakelijkheids- en proportionaliteitstoets te worden onderworpen. Als een Big Data analyse bijvoorbeeld uitwijst dat in de komende periode in een bepaalde wijk een verhoogd risico op inbraken bestaat, is op grond van zo'n toets dan voldoende te rechtvaardigen dat in die wijk meer surveillanceauto's zullen worden ingezet of zou zo'n inzet te zeer tot stigmatisering van de wijk leiden?

Binnen het veiligheidsdomein kunnen (semi-)geautomatiseerde processen zeker een nuttige rol spelen. De vraag is welke randvoorwaarden en eisen we stellen aan de verhouding tussen mens en machine, welke normen we hanteren. Het uiteindelijke doel is niet om automatische processen te verbieden maar deze aan door ons gestelde regels, normen en waarden te laten voldoen.

De WRR wijst in zijn rapport op verschillende situaties in het veiligheidsdomein waarin geautomatiseerde analyses en processen voorkomen. Naast de mogelijkheid om Big Data analyses te gebruiken voor het bepalen van de inzet van toezicht- of handhavingscapaciteit, noemt de WRR ook de mogelijkheid dat op basis van dergelijke analyses strafvorderlijke bevoegdheden zouden kunnen worden ingezet. Als de inzet daarvan zelf ook een onderdeel van het geautomatiseerde proces zou zijn, zou sprake zijn van geautomatiseerde besluitvorming met rechtsgevolgen, hetgeen verboden is.

Het inzetten van strafvorderlijke bevoegdheden is een goed voorbeeld van een risico bij semi-automatische besluitvorming. Voorkomen moet worden dat door de enkele aanwezigheid van een menselijke beslisser als "stempelmachine" het verbod op geautomatiseerde besluitvorming buiten toepassing blijft, terwijl het nemen van het desbetreffende besluit op alle inhoudelijke gronden overigens onder dat verbod zou vallen. Zoals ten behoeve van het strafrecht reeds is beschreven, zullen menselijke beslissers immuun moeten worden voor de suggestie dat de uitkomsten van computationele technieken noodzakelijkerwijs juist, volledig of zelfs maar relevant zijn in relatie tot verdachten.[14]

Bij andere voorbeelden, waarbij geen sprake is van een verboden geautomatiseerd besluit, is denkbaar dat menselijke tussenkomst in de vorm van validatie van de analyse of nadere weging van de uitkomst voordat een beslissing wordt genomen, niet noodzakelijk is. In de eerste plaats is bij de beoordeling hiervan van belang welke impact de Big Data analyse en het daaruit voortvloeiende gevolg op betrokkenen hebben. Is die impact klein, dan zal menselijke tussenkomst veelal niet noodzakelijk zijn. Wordt die impact groter, dan zal ook de noodzaak van menselijke tussenkomst snel toenemen. Wanneer sprake is van een beslissing die niet op individuen maar op groepen gericht is, kunnen andere of aanvullende voorwaarden nodig zijn. Een van de randvoorwaarden die dan moet gelden, is dat er geen sprake is van het onrechtmatig bevoor- of benadelen van bepaalde groepen door bijvoorbeeld toezicht onevenredig zwaar op één groep te richten. Er dient bovendien in dat soort situaties altijd ruimte te zijn om de Big Data analyse niet te volgen en de blik ook te richten op groepen die niet in het profiel vallen. Als dit soort gevolgen mogelijk zijn, is dus altijd een vorm van betekenisvolle menselijke tussenkomst nodig.

---

[14] M. Hildebrandt, Data-gestuurde intelligentie in het strafrecht. In: Homo Digitalis, Handelingen van de Nederlandse Juristen Vereniging. 146e jaargang, 2016/I, blz. 186.

Daarnaast kan de factor tijd, in combinatie met de zwaarte van de te nemen maatregel en de impact daarvan op de betrokkenen, een rol spelen. Wanneer op basis van Big Data analyses een mogelijk acuut veiligheidsprobleem wordt vastgesteld, kan de politie beslissen ter plaatse te gaan kijken. Het is dan niet wenselijk, en ook niet nodig, om de analyse eerst door een mens te laten controleren. Als de analyse bij aankomst van de politie onjuist blijkt te zijn, is er in dit soort situaties letterlijk en figuurlijk geen man overboord. Mocht zich dat vaker voordoen, dan kan er wel aanleiding zijn de gebruikte algoritmen nog eens kritisch tegen het licht te houden.

Rechtsbescherming
Naarmate de gevolgen van (semi-)geautomatiseerde besluiten op basis van Big Data technieken op het terrein van de veiligheid voor individuen groter zijn, is het daarnaast noodzakelijk dat er conform artikel 13 EVRM te allen tijde een daadwerkelijk en effectief rechtsmiddel is voor de betrokkenen die in hun belangen zijn geraakt. Daar ligt een belangrijke relatie met de transparantie en de reproduceerbaarheid van de gegevensanalyse. Om de juistheid van de beslissing te laten toetsen door een mens, is immers noodzakelijk dat achteraf kan worden vastgesteld hoe de gegevensanalyse is uitgevoerd. Het kabinet zal in dit verband 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.[15]

Aanbeveling 2 in § 6.4.5: De WRR beveelt aan dat het principe dat de verantwoordelijkheid voor de juistheid van Big Data processen te allen tijde bij de gegevensverwerkende partij blijft liggen, juridisch verankerd wordt. Deze dient aan te tonen waar een beslissing op gebaseerd is en welke factoren en wegingen daarin zijn meegenomen.

Het principe dat de verantwoordelijkheid voor de juistheid van Big Data processen te allen tijde bij de gegevensverwerkende partij blijft liggen, wordt verankerd in artikel 5, eerste lid, onder a, van de AVG, en artikel 4, eerste lid, onder a, van de Richtlijn. Daarin wordt bepaald dat de verwerking van persoonsgegevens rechtmatig en behoorlijk, respectievelijk eerlijk dient te zijn. Dat de verantwoordelijke zal moeten kunnen aantonen waarop een beslissing is gebaseerd en welke factoren en wegingen daarin zijn meegenomen, vloeit voort uit artikel 14, tweede lid, onder g, van de AVG, waarin is vastgelegd dat betrokkenen recht hebben op informatie over het bestaan van geautomatiseerde besluitvorming, met inbegrip van profilering, en nuttige informatie over de onderliggende logica, alsmede het belang en de verwachte gevolgen van die verwerking voor de betrokkene.

Aanbeveling 1 in § 6.5: De toegenomen mogelijkheden om data te verzamelen, dienen gepaard te gaan met een versteviging van het onafhankelijke toezicht. Voor het toezicht op de inlichtingendiensten zou, gelet op de taak van de CTIVD inzake bescherming van fundamentele rechten, de introductie van doorzettingsmacht/de mogelijkheid bindende (on)rechtmatigheidsoordelen te vellen gepast zijn.

Het kabinet deelt de mening van de WRR dat de toegenomen mogelijkheden om data en persoonsgegevens te verzamelen vragen om een versteviging van het onafhankelijk toezicht. Het breed gedragen besef dat de snelle technologische

[15] Zie ook: A.R. Lodder e.a., Big Data, Big Consequences – WODC 2014, blz. 47-56.

ontwikkelingen om een stevig regelgevend kader vragen heeft dan ook geleid tot het aannemen van de AVG en de Richtlijn gegevensbescherming opsporing en vervolging, waarmee onder andere wordt voorzien in een versteviging van de bevoegdheden en middelen van de Autoriteit Persoonsgegevens. Het ministerie van Veiligheid en Justitie en de Autoriteit Persoonsgegevens zijn een traject gestart waarin een onafhankelijk adviesbureau de consequenties daarvan in kaart brengt voor de capaciteit en het budget van de Autoriteit.

Op 28 oktober jl. is bij de Tweede Kamer een voorstel ingediend voor een nieuwe Wet op de inlichtingen- en veiligheidsdiensten ter vervanging van de huidige wet uit 2002. Versterking van het toezicht op de inlichtingen- en veiligheidsdiensten is een van de belangrijkste aspecten van het wetsvoorstel. Zo voorziet het wetsvoorstel bij de inzet van bepaalde bijzondere bevoegdheden in een voorafgaande, bindende toets door een onafhankelijke commissie met een rechterlijke en technische achtergrond, de Toetsingscommissie inzet bevoegdheden (TIB). Verder gaat de CTIVD fungeren als zelfstandige klachtinstantie die bindende uitspraken kan doen over klachten van burgers.

Aanbeveling 2 in § 6.5: De WRR beveelt aan om de transparantie van de gegevensverwerking te vergroten, en een beter evenwicht te zoeken tussen het vereiste van geheimhouding en het belang van openbaarheid over de uitvoering van staatstaken die aan fundamentele vrijheden raken.

Transparantie kan in belangrijke mate bijdragen aan "accountability" en vormt dan ook een basisprincipe in de AVG (art. 5 , eerste lid, onder a, en tweede lid). Het kabinet hecht op twee niveaus grote waarde aan dit principe bij het uitvoeren van Big Data analyses door overheidsorganisaties.

In eerste instantie betreft dat de mogelijkheid voor de samenleving om op geaggregeerd niveau te weten wanneer (persoons)gegevens betrokken worden in geautomatiseerde gegevensanalyses, en voor welk doel. De WRR wijst er bijvoorbeeld op dat veel relevante informatie over gegevensverwerkingen binnen samenwerkingsverbanden op het terrein van fraudebestrijding al beschikbaar is via convenanten en besluiten, maar dat deze niet erg toegankelijk zijn. Het kabinet acht het van belang om de transparantie over gegevensverwerkingen zo groot mogelijk te laten zijn, bijvoorbeeld door via websites van organisaties betrokkenen in meer algemene zin over het doel van de desbetreffende analyses te informeren en daarbij, voor zover mogelijk, aan te geven welke databestanden daarvoor worden gebruikt. Dan zijn betrokkenen op indirecte wijze in staat te beoordelen of in deze analyses mogelijk ook persoonsgegevens over hen worden betrokken. Het kabinet zal stimuleren dat organisaties een en ander op een voor de burger toegankelijke wijze in hun privacystatements opnemen.

Daarnaast betreft het transparantie over de wijze waarop Big Data analyses in concrete gevallen plaats vinden. In de kern gaat het om analyses met zodanig grote hoeveelheden gegevens, snelheid en diversiteit, dat er zeer complexe algoritmen nodig zijn om tot optimale resultaten te komen. Bij minder complexe analyses kan de juistheid van de uitkomsten makkelijker gecontroleerd worden, bijvoorbeeld door aan de desbetreffende persoon of organisatie gericht vragen te stellen. Iets soortgelijks moet bij het controleren van Big Data analyses ook mogelijk worden gemaakt: de juistheid van de analyse moet altijd in twijfel getrokken kunnen worden, bijvoorbeeld in juridische procedures. Bij Big Data

analyses is de analyse echter veel lastiger te doorgronden en kunnen discriminatie en negatieve profilering optreden. Het belang van transparantie is daarom nog groter dan bij vele andere (eenvoudiger) gegevensverwerkingen. Immers, om het handelen van de overheid te kunnen controleren, is het in deze gevallen bij uitstek noodzakelijk om inzicht te kunnen geven in de wijze waarop gegevens zijn betrokken in een analyse, en hoe de uitkomst van de analyse tot stand is gekomen. Dit is met name, maar niet uitsluitend, het geval wanneer analyses concrete gevolgen hebben voor personen van wie gegevens zijn verwerkt. Het komt hier in feite neer op het geven van inzicht in de gebruikte algoritmen, toetsbaarheid en transparantie van de gebruikte technologie en open validatie over de juistheid van de oorspronkelijke (bron) data waarop uitkomsten van analyses worden gebaseerd.

Dat degene die verantwoordelijk is voor de analyse en de daarop gebaseerde beslissing zal moeten kunnen aantonen waarop deze beslissing is gebaseerd en welke factoren en wegingen daarin zijn meegenomen, vloeit voort uit artikel 14, tweede lid, onder g, AVG, waarin is vastgelegd dat betrokkenen recht hebben op informatie over het bestaan van geautomatiseerde besluitvorming, met inbegrip van profilering, en nuttige informatie over de onderliggende logica, alsmede het belang en de verwachte gevolgen van die verwerking voor de betrokkene. Hierbij moet worden bedacht dat het vaak niet mogelijk zal zijn deze onderliggende logica te reproduceren. Dat geldt met name in gevallen waarin gebruikt wordt gemaakt van artificiële intelligentie. In dat geval is het van des te groter belang dat er voldoende mogelijkheden zijn om de uitkomst van de analyse zo nodig bij te stellen. Een equivalent van genoemde bepaling uit de AVG ontbreekt in de Richtlijn. In het kader van de implementatie daarvan zal worden bezien of een bepaling als deze niet ook voor geautomatiseerde besluitvorming op grond van strafrechtelijke gegevens zou moeten gaan gelden. Voor de transparantie rond Big Data analyses is verder van belang dat de overheidsorganisatie die verantwoordelijk voor de verwerking van persoonsgegevens ten behoeve van de analyse is, ingevolge de AVG en de Richtlijn een register van verwerkingsactiviteiten dient bij te houden (art. 30, resp. 24). Dit register dient onder meer de verwerkingsdoeleinden te bevatten, alsmede een beschrijving van de categorieën van betrokkenen, van de categorieën van persoonsgegevens en de categorieën van ontvangers aan wie de persoonsgegevens zijn of zullen worden verstrekt.

In voorkomende gevallen is het noodzakelijk om (delen van) de gegevensverwerking niet inzichtelijk te maken. Dit kan nodig zijn om te voorkomen dat personen zich kunnen onttrekken aan een effectieve taakuitoefening door de overheid. Inzicht in de gebruikte analysemethode kan immers aanleiding zijn om het gedrag bewust zodanig aan te passen dat men in de gegevensanalyse buiten zicht blijft. Daarnaast kan geheimhouding nodig zijn omdat inzicht in de gegevensverwerking raakt aan de nationale veiligheid. Het kabinet is van oordeel dat deze mogelijkheid zal moeten blijven bestaan, maar dat zij terughoudend dient te worden toegepast. Extern toezicht op deze vormen van gegevensverwerking, alsmede op de beslissing om (delen van) deze gegevensverwerking niet aan de openbaarheid prijs te geven, zal daarbij altijd aangewezen zijn.

Aanbeveling 3 in § 6.5: De WRR is van mening dat de mogelijkheden voor rechterlijke toetsing van wetgeving en beleid omtrent Big Data-toepassingen verbeterd moeten worden.

In reactie op deze aanbeveling wijst het kabinet allereerst op de bevoegdheden die de Nederlandse rechter nu reeds heeft om Big Data toepassingen te toetsen. De rechter kan formele wetgeving toetsen op verenigbaarheid met internationale mensenrechtenverdragen, zoals het EVRM, en aan het recht van de Europese Unie, voor zover het gaat om de toepassing daarvan (bijv. de Privacyrichtlijn). Lagere regelgeving en beleid kan de rechter toetsen aan alle hogere bronnen van recht, zoals verdragen, de Grondwet en de Wet bescherming persoonsgegevens.

Verder is een nuancering op haar plaats, waar de WRR opmerkt dat de Nederlandse burger is aangewezen op een gang naar de Straatsburgse of Luxemburgse rechter omdat de Nederlandse rechter wetgeving niet kan toetsen wanneer (nog) niet van persoonlijke schade is gebleken. Ook voor de ontvankelijkheid van een klacht voor het Europese Hof voor de Rechten van de Mens moet een verzoeker, of een groep personen, stellen zelf slachtoffer te zijn van een schending van het verdrag (art. 34 EVRM). Bij het EHRM kan in beginsel niet worden geklaagd zonder dat de verzoeker kan aantonen dat hij een eigen, individueel of collectief nadeel heeft ondervonden. Tevens dienen de nationale rechtsmiddelen te worden uitgeput. En de prejudiciële vragen die het Hof van Justitie van de EU beantwoordt, vinden hun grondslag in een nationale rechtszaak. De gang naar de Straatsburgse of Luxemburgse rechter dient voorts niet te worden afgewacht: de Nederlandse rechter dient het Nederlandse recht verdragsconform en EU-rechtconform te interpreteren en moet dit op grond van artikel 94 Grondwet ook buiten toepassing laten indien het strijdig is met eenieder verbindende verdragsbepalingen. Bij twijfel over de uitleg van het EU-recht kunnen vraagstukken door de Nederlandse rechter als prejudiciële vraag aan het Hof van Justitie van de EU worden voorgelegd.

De WRR lijkt zich vooral te richten op het vergroten van de mogelijkheden voor burgers die zich zorgen maken over de maatschappelijke effecten van Big Data toepassingen, om zich tot de rechter te wenden. De WRR stelt dat het klachtrecht in de huidige situatie sterk verbonden is aan individuele schade en dat de mogelijkheden voor collectieve procedures bij de rechter gebonden zijn aan de criteria van artikel 3: 305a van het Burgerlijk Wetboek. Dit geeft, aldus de WRR, 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 kabinet begrijpt deze zorgen en overwegingen en is dan ook bereid nader te onderzoeken of uitbreiding van de mogelijkheden voor burgers en belangenorganisaties om besluitvorming en wetgeving over Big Data toepassingen te laten toetsen door de rechter mogelijk en wenselijk is.

Aanbeveling 4 in § 6.5: De WRR adviseert de regering de voorbereidingen van adequate wetgeving zoveel mogelijk in EU-verband te entameren. De Europese Unie zal internationale normering effectiever kunnen bevorderen dan afzonderlijke lidstaten. Daarnaast zal de Nederlandse regering kunnen bevorderen dat het onderwerp Big Data bij de Raad van Europa hogere prioriteit krijgt.

Met het oog op de voorbereiding van wetgeving ter uitvoering van de AVG en de Richtlijn heeft Nederland contacten met andere lidstaten en wordt deelgenomen aan bijeenkomsten daarover teneinde tot zo uniform mogelijke uitvoeringswetgeving te komen. Nu de AVG en de Richtlijn nog maar zo kort geleden na langdurige onderhandelingen tot stand zijn gekomen, acht het kabinet het niet opportuun om op het terrein van gegevensbescherming

nieuwe regelgeving in EU-verband te entameren. Wel beziet het, zoals eerder gezegd, mogelijkheden om binnen de ruimte die de AVG en de Richtlijn bieden, in de Nederlandse wetgeving nadere regels over het gebruik van data-analyse op te nemen.

Binnen de Raad van Europa werd van 2012 tot en met juni 2016 onderhandeld over de modernisering van het huidige Dataprotectieverdrag (Conventie 108) van de Raad van Europa. Deze Conventie 108 legt een aantal beginselen ter bescherming van persoonsgegevens vast en bestrijkt alle maatschappelijke sectoren, ook die van de inlichtingen- en veiligheidsdiensten. De onderhandelingen over de tekst van de Conventieverdrag werden op 16 juni 2016 afgerond. Doel van de modernisering van dit dataprotectieverdrag is dat het adequate bescherming binnen een toekomstbestendig kader biedt. Het verdrag zal Big Data verwerkingen in alle maatschappelijke sectoren normeren, waaronder ook de sectoren met taken en bevoegdheden op het terrein van de veiligheid. Het kabinet heeft de ambitie van de Raad van Europa om ook landen van buiten de Raad toe te laten bij dit verdrag, steeds ten volle ondersteund met het oog op een verspreiding van een zo hoog mogelijke standaard van dataprotectie. 48 landen hebben inmiddels het huidige Dataprotectieverdrag ondertekend, waaronder Marokko, Uruguay, Mauritius en Tunesië. Deze benadering zal, zo is de uitdrukkelijke wens van alle partijen, leiden tot een hoge globale standaard van dataprotectie buiten de grenzen van de Raad van Europa. Met deze ambitie vormt het Dataprotectieverdrag een aanvulling op de AVG en de Richtlijn gegevensbescherming opsporing en vervolging, die in beginsel alleen op het grondgebied van de EU gelden.