Bijlage 2. Reactie op de afzonderlijke reguleringsopties in het rapport ´Modernisering procesrecht in het licht van big data´

Het onderhavige onderzoek is uitgevoerd door de Universiteit van Tilburg in opdracht van het WODC (ministerie van Justitie en Veiligheid). In het onderzoek is gekeken welke aanpassingen aan het (proces)rechtelijk kader zouden kunnen worden gedaan om de rechtspositie van burgers (verder) te borgen in het licht van grote dataverwerkingsprocessen, meer specifiek ook met het oog op de mogelijkheid om op te komen voor een collectief of algemeen belang. Met dit onderzoek is uitvoering gegeven aan de motie van het lid Buitenweg.[1]

In de brief, waar deze bijlage onderdeel van uitmaakt, geeft het kabinet in meer algemene zin aan welke conclusies het trekt uit het onderhavige onderzoek. In deze bijlage wordt gereageerd op de afzonderlijke reguleringsopties.

Reguleringsopties I: stel regelgeving vast waarin data, niet zijnde persoonsgegevens, worden beschermd.

In reguleringsoptie I wordt aangekaart dat big data processen niet altijd gaan over persoonsgegevens, maar om grote hoeveelheden geaggregeerde - en daarmee vaak anonieme - data. De geanonimiseerde datasets en de analyse daarvan vallen dan buiten de kaders van de Algemene Verordening Gegevensbescherming (AVG). De onderzoekers signaleren dat dit twee lacunes in het wettelijk kader oplevert. Ten eerste dat een beslissing die wordt genomen op basis van een anonieme dataset alsnog grote impact kan hebben op individuen, bijvoorbeeld bij het opstellen van risicoprofielen voor bepaalde wijken. Ten tweede is data steeds minder stabiel, door anonimiseren of pseudonimiseren kan data in een 'split-second' worden omgeturnd van persoonsgegevens in niet-persoonsgegevens. Organisaties investeren mede met dat doel indachtig in het anonimiseren van gegevenssets.

De onderzoekers stellen daarom voor om een minimumstandaard neer te leggen voor de verwerking van alle data, waarbij een aantal verwerkingsprincipes in acht moeten worden genomen ongeacht of er persoonsgegevens worden verwerkt. Hier zou uitvoering aan kunnen worden gegeven door een aantal beginselen uit de AVG ook van toepassing te verklaren op niet-persoonsgegevens.

Ten aanzien van de eerste door de onderzoekers geïnventariseerde lacune steunt het kabinet de redenering dat het gegevensbeschermingsrecht geen directe bescherming biedt wanneer geen persoonsgegevens worden verwerkt, terwijl er weldegelijk gevolgen kunnen zijn voor individuen of groepen. Daarbij wil het kabinet wel opmerken dat het van oordeel is dat in veel gevallen waar risico´s bestaan voor burgers bij een analyse van gegevens, er al snel sprake zal zijn van de verwerking van persoonsgegevens. Dit komt mede zoals de onderzoekers ook aanhalen, door de brede definitie en uitleg van het begrip ´persoonsgegevens´. Dit laat onverlet dat het kabinet ziet dat de in het rapport geschetste scenario´s over data-analyse waarbij de bescherming van de AVG ontbreekt, weldegelijk relevant zijn.

Het is daarbij van belang om vast te stellen dat het niet zo is dat de burger in dergelijke scenario´s geen juridische bescherming geniet. De toepassing van data-analyse door de overheid is altijd ter uitvoering van een overheidstaak of wettelijke bevoegdheid of verplichting. Dit maakt al dat het verwerken van de gegevens in kwestie wel genormeerd is. Het ontbreken van de beschermende normen uit de AVG laat onverlet dat de algemene normen en rechtsbeginselen

[1] In de motie werd de regering gevraagd om in verband met dataverwerkingsprojecten die de belangen van individuen overstijgen de mogelijkheden voor het verruimen van collectieve procedures bij de rechter te onderzoeken en de Kamer hierover te informeren. Zie Kamerstukken II 2017/18, 32761 nr. 119.

waar deze normen uitdrukking geven ook buiten de AVG een brede gelding hebben, zeker voor zover dit de overheid betreft. Deze zijn gecodificeerd in de Algemene Wet Bestuursrecht (Awb) en gelden op grond van het Burgerlijk Wetboek (BW) ook voor privaatrechtelijk handelen van de overheid. Belangrijk voorbeeld daarvan is het motiveringsbeginsel, wat meebrengt dat altijd inzichtelijk moet zijn waarom een besluit genomen is (ook als dat uit gegevens voortvloeit die geen persoonsgegevens zijn).[2] Hoewel de artikelen niet direct van toepassing zijn op feitelijk overheidshandelen wordt algemeen aangenomen dat het een beginsel van de democratische rechtsstaat is dat een bestuursorgaan over al het handelen verantwoording af moet kunnen leggen en in die zin transparant is. Hierbij komt dat ook via het civiele recht mogelijkheden zijn om onrechtmatig handelen aan de rechter voor te leggen, ook indien er geen persoonsgegeven worden verwerkt.

Voorts is van belang nog maar eens te benadrukken dat grondrechten ook online gelden.[3] Dit betekent dat ook als er geen persoonsgegevens worden geanalyseerd, een betrokkene zich wel kan beroepen op normen uit bijvoorbeeld het Europees Verdrag van de Rechten van de Mens (EVRM), zoals het recht niet te worden gediscrimineerd of het recht op privéleven, indien deze rechten worden geschonden.[4] Waar deze bepalingen jegens de overheid direct kunnen worden ingeroepen, geldt dat deze rechten ook (indirecte) horizontale werking kunnen hebben (tussen burgers en bedrijven onderling).[5] Daarmee is dus zowel jegens de overheid als het bedrijfsleven een zekere bescherming geboden.

Desalniettemin merkt het kabinet op dat de burger zich vaak pas op de - naast de AVG - geldende beschermende kaders kan beroepen als er reeds iets mis is gegaan (er is bijvoorbeeld op onrechtmatige wijze een besluit genomen, een inbreuk op een fundamenteel recht gemaakt of er is schade geleden). De AVG expliciteert rechtsbeginselen en fundamentele rechten en legt partijen verplichtingen op die transparantie en zorgvuldigheid bevorderen. Deze expliciete informatie- en transparantieverplichtingen die de AVG biedt spelen een centrale rol in het voorkomen van mensenrechtenschendingen in de digitale context, bijvoorbeeld omdat discriminatie eerder aan het licht komt door goede transparantieverplichtingen.[6] Hiermee worden onrechtmatige gegevensverwerkingen dus ook aan de ´voorkant´ voorkomen. Deze belangrijke AVG-normen gelden niet ten aanzien van analyses van niet-persoonsgegevens die weldegelijk impact op burgers kunnen hebben. Het kabinet ziet dan ook waarom de onderzoekers in overweging geven te bezien of ook ten aanzien van niet-persoonsgegevens bepaalde zorgvuldigheidsnormen of transparantieverplichtingen zouden kunnen worden vastgesteld.

Het kabinet is echter van mening dat het vaststellen van regelgeving voor het verzamelen van alle typen gegevens te veel omvattend is en zou leiden tot overregulering. De vraag zou daarbij rijzen welk belang precies beschermd moet worden en hoe deze regelgeving zich zou verhouden tot bovengenoemde reeds geldende beginselen uit de Awb. Waar het kabinet geen heil ziet in het creëren van wetgeving voor alle gegevens, zet het wel stappen om de door de onderzoekers geïdentificeerde lacune op te vullen door in te zetten op aanvullende eisen aan bepaalde (algoritmische) data-analyses en de communicatie daarover. Dit omdat het kabinet constateert dat de problematiek vooral gelegen is in het ontbreken van een aantal expliciete eisen uit de AVG en de Awb ten aanzien van zorgvuldigheid bij – en transparantie over –analyses, waar die weldegelijk impact hebben op burgers.

Allereerst wijst het kabinet daarbij op de brief over waarborgen tegen de risico´s van data-analyse door de overheid. Daarin is aangekondigd dat er wordt gewerkt aan aanvullende richtlijnen voor data-analyse door de overheid.[7] Middels deze richtlijnen poogt het kabinet de eisen die

[2] Zoals vervat in 3:46 en 3:47 Awb. Zie ook: ECLI:NL:RVS:2017:1259, Raad van State, 17 mei 2017
[3] Kabinetsreactie op UU-rapport ´Algoritmes en grondrechten´, p. 3.
[4] Artikelen 14 en 8 EVRM.
[5] Reactie op commissiebrief inzake vragen n.a.v. kabinetsreactie op rapporten Rathenau instituut, 16 oktober 2018, p. 2.
[6] Kabinetsreactie op UU-rapport ´Algoritmes en grondrechten´, p. 4.
[7] Kamerstukken II 2018/19, 26 643, nr. 641.

voortvloeien uit de Awb en de AVG voor overheidsorganisaties nader te concretiseren. In bijlage 1.1 bij die brief is tevens al een eerste versie van deze richtlijnen opgenomen. In het eerste kwartaal van 2021 wordt bezien of deze waar nodig worden omgezet in wettelijke waarborgen. De richtlijnen richten zich in beginsel op data-analyse waarbij persoonsgegevens worden verwerkt, omdat daar vaak de grootste risico´s bestaan. Dit laat onverlet dat de neergelegde kwaliteits- en zorgvuldigheidseisen relevant zijn ook wanneer persoonsgegevens geen onderdeel zijn van de data-analyse. De richtlijnen zijn dan ook relevant voor data-analyse met rechtsgevolg voor burgers of die de burger in aanmerkelijke treft. Daarmee worden de benodigde zorgvuldigheidsnormen bij data-analyse door de overheid geconcretiseerd en vastgelegd. Voorts zijn in bijlage 1.2. bij de brief ook richtlijnen vastgesteld voor communicatie over data-analyse naar het publiek. Wanneer er concretere transparantie- en zorgvuldigheidsnormen gelden voor overheden betreffende de wijze waarop zij met gegevens, waaronder persoonsgegevens, omgaan, worden burgers beter in staat gesteld te overzien welke analyses worden uitgevoerd en waar nodig in te grijpen voor schade kan ontstaan.

Ten tweede is in dezelfde brief aangegeven dat het de voorkeur verdient om verdere regels voor data-analyse voor het bedrijfsleven in Europees verband af te spreken. De discussie hierover is door de Europese Commissie afgetrapt met het op 19 februari jl. gepubliceerde witboek AI. Hierin bespreekt de Commissie onder meer de mogelijkheid van een aanvullend wettelijk kader specifiek voor AI-toepassingen met een ´hoog risico´. Het kabinet heeft een appreciatie van het witboek gepubliceerd waarin het ingaat op de wenselijkheid van een dergelijk kader. Daarbij heeft het, mede naar aanleiding van het door de onderzoekers opgebracht punt, naar voren gebracht dat eventuele specifieke aanvullende regels voor toepassing met ´hoog risico´ van nut kunnen zijn in aanvulling op de waarborgen uit de AVG. Voordeel van deze risico-gebaseerde benadering is dat er in Europees verband regels kunnen worden vastgesteld voor het toepassen van data-analyse, mogelijk geldend voor zowel het bedrijfsleven als overheid, waarmee het risico op negatieve impact op burgers wordt beperkt. Dergelijke regels zouden ook kunnen gelden waar geen persoonsgegevens worden verwerkt. Naar verwachting komt de Europese Commissie in het voorjaar van 2021 met een eerste voorstel.

De tweede geïnventariseerde lacune, over het anonimiseren van datasets, maakt het aangekaarte probleem over het ontbreken van AVG waarborgen bij bepaalde gegevenssets relevanter. De onderzoekers merken immers op dat organisaties veel investeren om gegevens aan het regime van de AVG te onttrekken door deze te anonimiseren. Daarover wil het kabinet opmerken dat het anonimiseren van gegevenssets in principe als iets positief ziet. Door de inzet van anonimiseringstechnieken en andere *privacy enhancing technologies* (PET) als ´differential privacy worden privacyrisico´s gemitigeerd.[8] Het kabinet is daarom voornemens de inzet van PET actiever te stimuleren. Daarbij wordt bijvoorbeeld gedacht aan het identificeren van goede praktijkvoorbeelden bij overheidsorganisaties om deze vervolgens ook in andere organisaties te introduceren, maar ook door te bezien hoe de toepassing van PET concreter kan worden verbonden aan de relevante begrippen uit de AVG.

Zoals de onderzoekers schetsen is het anonimiseren echter problematisch als een set gegevens daarmee (bewust) aan het beschermende regime van de AVG wordt onttrokken, maar er wel risico´s blijven bestaan voor burgers en hun fundamentele rechten. Wat dat betreft heeft het kabinet hierboven reeds de lopende actielijnen uiteengezet om die lacune te dichten. Als er voldoende waarborgen bestaan bij de analyse van niet-persoonsgegevens mét impact op burgers, is het ook van minder belang dat gegevenssets worden geanonimiseerd en daarmee aan de reikwijdte van de AVG worden onttrokken. In dat geval worden de positieve effecten van anonimisering benut, zonder rechtsbescherming uit te hollen. Dit alles in overweging nemend ziet het kabinet effectievere en toegankelijkere anonimiseringstechnieken dan ook als een positieve ontwikkeling voor de bescherming van persoonsgegevens.

[8] Hierbij wordt een model ingezet om inzichtelijk te maken hoeveel ´ruis´ aan een dataset moet worden toegevoegd om herleiding onmogelijk te maken, maar de accuraatheid van de dataset te behouden als deze wordt ingezet voor analyse.

Opmerking verdient nog dat het begrip ´anonimisering´ uit de AVG strikt wordt uitgelegd.[9] Dit betekent dat er in de praktijk vaak sprake is van pseudonimisering, waarbij de gegevens versleuteld zijn en voor de verwerkingsverantwoordelijke nog wél te herleiden zijn. In dat geval zijn de gegevens in kwestie nog steeds ´persoonsgegevens´ en gelden de waarborgen uit de AVG. Daarbij komt dat er dusdanig veel informatie van individuen (vrij) beschikbaar is, of wordt verzameld door verwerkingsverantwoordelijken, dat er door combinatie van verschillende datasets vaak herleiding mogelijk is. In die gevallen is de AVG dus wél van toepassing.

Het kabinet benadrukt dat het begrip ´persoonsgegeven´ meebeweegt met de stand van de techniek. De AVG bevat een zogeheten ´redelijkheidstest´ die voorschrijft dat moet worden bezien of gegevens ´redelijkerwijs´ kunnen worden herleid tot een individu (met in acht name van de beschikbare middelen om gegevens te herleiden). Indien dat het geval is spreken we van ´persoonsgegevens´. Door nieuwe technologische ontwikkelingen verandert de invulling van de vraag of gegevens ´redelijkerwijs´ kunnen worden herleid tot een individu, omdat de beschikbaarheid van nieuwe technieken mee verandert. Daarmee verandert, gelet op bovenstaande conclusies die het kabinet trekt, ook het beschermingsniveau bij gegevensverwerkingen. Het kabinet vind het dan ook van groot belang om nader in kaart te brengen hoe de veranderende stand van de techniek van invloed is op de AVG en rechtsbescherming in brede zin en zal hier nader onderzoek naar laten verrichten.

Reguleringsoptie II : reguleer het analyseren van data

In reguleringsoptie II wordt de optie voorgelegd om de analysefase van data verder te reguleren. Dit werd eerder ook benoemd in het rapport van de WRR over big data.[10] Voornaamste argument hiervoor is dat de analysefase nooit volledig neutraal is, het perspectief van alle betrokkenen bepaalt deels de analyse en dus de uitkomsten. Hoewel de analyse van big data vaak plaatsvindt met niet-persoonsgegevens, zijn er wel degelijk consequenties voor degene die aan de analyse onderhevig zijn. Daarom stellen de onderzoekers voor om regelgeving en richtlijnen te maken voor de correcte uitvoering van data-analyses, hierbij kan bijvoorbeeld worden aangesloten bij de Praktijkcode voor Europese Statistieken.

Het kabinet ziet dat er in bepaalde gevallen behoefte is aan verdere waarborgen in de analysefase. Zoals het kabinet onder reguleringsoptie I al heeft benoemd zal de AVG vaak gelden bij data-analyse met risico´s voor burgers. In dat geval moet de verwerking van persoonsgegevens ingevolge artikel 5 AVG onder meer rechtmatig en behoorlijk zijn. Waar ´rechtmatigheid´ toeziet op naleving van de juridisch afgebakende vereisten zoals neergelegd in de AVG, omvat ´behoorlijkheid´ ook dat verwerkingen niet in strijd mogen zijn met fundamentele rechtsbeginselen. De conclusie dat de analysefase nu vrijwel ongereguleerd is kan het kabinet, zeker voor zover er persoonsgegevens worden verwerkt (zie optie 1), dan ook niet geheel onderschrijven.

Wél ziet het kabinet dat de bestaande normen verdere concretisering behoeven. Daarom zet het stappen om de waarborgen in de analysefase verder aan- en in te vullen. De onder reguleringsoptie I genoemde brief over ´de waarborgen tegen de risico´s van data-analyse door de overheid´ en bijbehorende set richtlijnen zijn daarvan het meest pregnante voorbeeld. De richtlijnen worden momenteel doorontwikkeld in samenwerking met een aantal publieke organisaties.[11] Ander spoor waarlangs het kabinet verkent of de analysefase verdere regulering

[9] Artikel 4 lid 1 AVG jo. overweging 26 bij de AVG definiëren wanneer een gegeven als persoonsgegeven moet worden gekwalificeerd. Relevante uitleg van de WP-29 Werkgroep (de voorganger van de EDPB) is te consulteren via: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf.
[10] Rapport ¨Big data in een vrije en veilige samenleving¨, Wetenschappelijke Raad voor het Regeringsbeleid (WRR), 2016.
[11] Kamerstukken II 2018/19, 26 643, nr. 641.

behoeft is het eerder genoemde witboek AI van de Europese Commissie. Het kabinet heeft in haar appreciatie aangegeven in beginsel positief te staan tegenover een aantal aanvullende regels voor hoog risico toepassingen.[12] Dit omvat mogelijk ook regels die raken aan de analysefase.

Waar bovengenoemde twee trajecten uit zouden kunnen monden in wetgeving, zet het kabinet ook andere (beleids-)instrumenten in om te bevorderen dat het voor ontwikkelaars makkelijk wordt om misstanden in de analysefase te voorkomen. Voorbeeld daarvan zijn de systeemprincipes voor AI-ontwikkelaars om discriminatie te voorkomen die momenteel door het Ministerie van BZK worden onderzocht. Hoewel dit de analysefase niet verder reguleert biedt het AI-ontwikkelaars wel concrete handvaten. Daarnaast onderzoekt het kabinet de mogelijkheid om, in aanvulling op bovengenoemde richtlijnen en de bestaande verplichtingen omtrent het uitvoeren van een gegevensbeschermingeffectenbeoordeling[13] (hierna: ¨DPIA¨), een zogeheten algoritme impact assessment (AIA) te introduceren. Hiermee zouden overheidsorganisaties conform de systematiek van de DPIA specifiek moeten evalueren of ingezette algoritmen voor data-analyse geen inbreuk maken op mensenrechten of anderszins tot onrechtmatigheid leiden.

Reguleringsoptie III: stel een horizonbepaling in voor big data projecten

In reguleringsoptie III stellen de onderzoekers dat er in zowel de publieke als private sector vaak hoge verwachtingen bestaan als het gaat om de inzet van big data-analyses, terwijl de concrete opbrengst van deze projecten tegen kan vallen. Zij wijzen op het voorstel uit het WRR-rapport over big data om bij dergelijke projecten in het veiligheidsdomein een vast evaluatiemoment in te stellen.[14] Bij een dergelijke evaluatie zal er op een vast moment in de tijd (3 tot 5 jaar) worden onderzocht of de noodzaak voor het project nog steeds bestaat en het gegevensverwerkingsproces effectief was en wordt er een kosten-batenanalyse gemaakt.[15]

De onderzoekers stellen verder dat er momenteel geen duidelijke en uniforme richtlijnen zijn voor het evalueren van Big Data projecten binnen de overheid. Ze stellen voor dat overheden verplicht een vast stramien moeten volgen bij het inzetten van big-data analyses waarbij zij eerst vaststellen wat de situatie is zonder inzet van deze toepassing. Vervolgens kunnen ze na 3 tot 5 jaar nogmaals meten of de inzet van de big-data analyse succesvol is, of dat deze stopgezet kan worden. De onderzoekers lijken hierbij een breder belang dan privacy van betrokkenen te verdedigen. Zo verwijzen ze naar het rapport van de Commissie-Elias waarin onder meer wordt gesteld dat veel ICT-projecten mislukken, mede ook omdat deze zakelijke rechtvaardiging missen.

Waar de onderzoekers stellen dat het kabinet in reactie op het WRR-rapport zich positief heeft uitgelaten over voorliggend voorstel om een evaluatietermijn vast te stellen[16], ligt dit genuanceerder. In de kabinetsreactie stelt het kabinet namelijk dat een vaste termijn van 3 tot 5 jaar minder goed bij de methodiek van een big-data project past.[17] Het kabinet is wel, net als de onderzoekers, van oordeel dat het periodiek evalueren van big-data toepassingen van belang is. Daarbij wil het aansluiten bij de bestaande systematiek van de AVG en de DPIA uit artikel 35 AVG.[18] De AVG schrijft tevens voor dat een dergelijke toetsing waar nodig herhaald moet worden, ook wanneer de gegevensverwerking niet verandert. De Autoriteit Persoonsgegevens raadt aan deze toetsing op zijn minst eens per drie jaar te herhalen.[19] Gelet op dat één van de centrale

[12] Kabinetsappreciatie ´Witboek kunstmatige intellgentie´, https://www.rijksoverheid.nl/documenten/kamerstukken/2020/04/20/kabinetsappreciatie-witboek-kunstmatige-intelligentie.
[13] Artikel 35 AVG.
[14] WRR Rapport 'Big data in een vrije en veilige samenleving', p. 14.
[15] Tweede Kamer vergaderjaar 2016-2017, 26 643, nr. 426 (bijlage), p. 11.
[16] Voorliggend rapport, p. 135.
[17] Bijlage bij de kabinetsreactie op het WRR Rapport ´Big data in een vrije en veilige samenleving´, p. 11.
[18] Tweede Kamer vergaderjaar 2016-2017, 26 643, nr. 426 (bijlage), p. 10.
[19] Zie https://www.autoriteitpersoonsgegevens.nl/nl/zelf-doen/data-protection-impact-assessment-dpia.

vragen in een DPIA betreft of de gegevensverwerking leidt tot verwezenlijking van het beoogde doel, zal daarbij weldegelijk aan de orde komen of het big-data project rendeert. Concreet betekent dit dus dat er reeds een evaluatiemoment bestaat. Het is daarbij aan de desbetreffende stuurgroep c.q. opdrachtgever van het project om te bepalen of de noodzaak nog bestaat, de doelen gehaald kunnen worden, en daarmee of het wenselijk en rechtmatig is om het project te continueren.[20]

Wat betreft de constatering van onderzoekers dat er geen vastomlijnd kader bestaat voor een dergelijke evaluatie wijst het kabinet op het Model gegevensbeschermingseffectenbeoordeling rijksdienst.[21] Indien een rijksoverheidsorganisatie, gelet op de geïdentificeerde risico´s, een DPIA uitvoert wordt dit gedaan aan de hand van dit vaste model. In dit stuk wordt, naast de specifieke risico´s van big-data toepassingen, ook gewezen op de *good practice* om de PIA om de drie jaar te evalueren.[22] Het model wordt het komend jaar geëvalueerd. Het kabinet zal daarbij, rekening houdend met deze aanbeveling van de onderzoekers, in het stuk tot uitdrukking brengen dat het doel van de verwerking, wil dat gerechtvaardigd zijn, een zo materieel mogelijke inhoud dient te hebben. Hiermee worden de overheidsorganisaties aangespoord om concrete en bij voorkeur meetbare doelen aan een gegevensverwerking te verbinden.

Reguleringsoptie IV: versterk het civielrechtelijk systeem door collectieve acties en algemeen belang acties eenvoudiger en effectiever te maken

De onderzoekers identificeren het civiele recht als het rechtsgebied dat de beste mogelijkheden biedt voor het voeren van acties in het collectief of algemeen belang. Teneinde dit nog verder uit te breiden stellen ze een aantal aanpassingen voor.

Allereerst benoemen de onderzoekers dat het aantal collectieve acties zowel in het bestuurs- als civiele recht beperkt wordt door het vereiste dat de vertegenwoordigende rechtspersoon in kwestie ´feitelijke werkzaamheden´ uit moet voeren die een link hebben met het te beschermen belang, hetgeen de procesmogelijkheden voor dergelijke rechtspersonen beperkt. De onderzoekers wijzen erop dat dit is gecodificeerd in artikel 1:2 lid 3 van de Algemene wet bestuursrecht (Awb) en artikel 3:305a Burgerlijk Wetboek (BW). Ten aanzien van het BW concluderen de onderzoekers dat het vereiste van ´feitelijke werkzaamheden´ volgt uit de relevante jurisprudentie op dat gebied. Het kabinet benadrukt dat, wat betreft de collectieve vordering in het civiele recht, feitelijke werkzaamheden geen vereiste zijn. Dit wordt in het rapport tevens benoemd.[23] Feitelijke werkzaamheden kunnen wel een indicatie zijn dat de rechtspersoon in kwestie voldoende expertise heeft en dat daarmee is gewaarborgd dat de rechtspersoon de belangen van de personen ten behoeve van wie de rechtsvordering is ingesteld kan behartigen. Gelet op dat beperking ten aanzien van feitelijke werkzaamheden dus niet zo absoluut is in het civiele recht, en dat de onderzoekers teven concluderen dat deze beperking niet als stringent wordt beschouwd in de literatuur en door geïnterviewden, ziet het kabinet geen aanleiding om een aanpassing van de eisen te overwegen.

Hieraan gelieerd merken de onderzoekers op dat zij voorzien dat procesmogelijkheden voor rechtspersonen in het algemeen belang beperkt kunnen zijn, omdat een big data proces kan leiden tot een gelijktijdige schending van meerdere mensenrechten, waar rechtspersonen zich wellicht (statutair) slechts richten op één specifiek mensenrecht. Het kabinet begrijpt de zorg van de onderzoekers dat dit zou kunnen leiden tot niet- of gedeeltelijke ontvankelijkheid van de rechtspersoon, maar is van oordeel dat de gestelde eisen niet dusdanig specifiek zijn dat er snel

[20] Tweede Kamer vergaderjaar 2016-2017, 26 643, nr. 426 (bijlage), p. 11.
[21] https://www.rijksoverheid.nl/documenten/rapporten/2017/09/29/model-gegevensbeschermingseffectbeoordeling-rijksdienst-pia.
[22] Idem, pp. 10-12.
[23] Te vinden op p. 216 van onderhavig rapport.

sprake zal zijn van niet-ontvankelijkheid bij schending van meerdere mensenrechten in een big-data context. Het is voorts aan de rechtspersoon zelf om te bepalen hoe smal of breed de reikwijdte is van de doelen waarvoor hij op wil komen.

Ten tweede stellen de onderzoekers voor het verplichte vooroverleg uit artikel 3:305a lid 2 BW te schrappen of beperken teneinde te voorkomen dat rechtspersonen niet-ontvankelijk worden verklaard. Het vooroverleg is wat het kabinet betreft een nuttig en belangrijk onderdeel van de regeling voor collectieve acties, dat ook door een aantal bij het rapport betrokken partijen als nuttig wordt ervaren. Het ziet geen aanleiding het vooroverleg te beperken nu het vooroverleg de implementatie is van een Europese richtlijn en termijn voor vooroverleg is beperkt tot twee weken.[24] Ook uit onderhavig onderzoek komt niet naar voren dat dit in de praktijk een barrière opwerpt die voor problemen zorgt.

Ten derde benoemen de onderzoekers dat een grote barrière bij het voeren van acties in het collectief en algemeen belang is gelegen in de bijbehorende kosten. Daartoe stellen de onderzoekers twee opties voor.

Als eerste optie stellen de onderzoekers dat belangrijk is dat er ruim baan wordt geven aan zogeheten ´opt-out procedures´. Zij stellen daarbij al vast dat Nederland de laatste jaren grote stappen heeft gezet op dit gebied, specifiek met de Wet Afwikkeling Massaschade in Collectieve Actie (WAMCA) die per 1 januari 2020 in werking is getreden. De wet regelt dat er één exclusieve belangenbehartiger wordt aangewezen. Wanneer dit plaats heeft gevonden kunnen gedupeerden zich aan de collectieve belangenbehartiging onttrekken door een ´opt-out´. De uitspraak is vervolgens bindend voor alle gedupeerden die zich niet expliciet hebben onttrokken aan het proces. Voor zover er geen sprake is van een situatie zoals vervat in artikel 37 UAVG, kan er dus een collectieve procedure met opt-out systeem worden gevoerd om via het civiele recht schadevergoeding te vorderen voor onrechtmatige verwerking van persoonsgegevens. Het kabinet ziet daarmee, net als de onderzoekers, dat er voldoende ruimte wordt gegeven aan gewenste opt-out procedures in het civiele recht, ook in de context van big data processen.

Relevant is nog te vermelden dat het kabinet signaleert dat er recent meer civiele zaken worden gestart waarbij schadevergoeding wordt geëist voor een schending van bepalingen uit de AVG. Dit omvat mede collectieve procedures.[25] Dit sterkt het kabinet voorlopig in zijn conclusie dat er voldoende ruimte wordt gegeven aan opt-out procedures. Het kabinet zal deze ontwikkeling nauwgezet blijven volgen om te bepalen of enige verruiming toch noodzakelijk kan zijn. Relevant om te vermelden is dan ook dat er recent overeenstemming tussen de Raad en het Europees Parlement is bereikt over een nieuwe Europese Richtlijn betreffende het voeren van collectieve actie procedures. In deze Richtlijn worden opt-out procedures nadrukkelijk toegestaan.

Als tweede voeren de onderzoekers aan dat de schadevergoeding voor een onrechtmatige daad in Nederland vaak relatief laag is, specifiek wanneer het gaat om immateriële schade. Schendingen van de AVG, of andere voor big data processen relevante kaders, zullen veelal uitmonden in immateriële schade. Deze schade is lastig vast te stellen en wordt volgens de onderzoekers in Nederland traditioneel laag begroot. De onderzoekers stellen voor om een vaste bedragen voor immateriële schade vast te stellen.

Immateriële schade komt naar Nederlands recht onder meer voor vergoeding in aanmerking, als er sprake is van (i) lichamelijk letsel, (ii) aantasting van de eer of goede naam of (iii) de benadeelde op andere wijze in zijn persoon is aangetast (artikel 6:106, lid 1, onder b, Burgerlijk Wetboek). Bij onzorgvuldig handelen dat big data betreft, zijn de laatste twee genoemde

[24] Richtlijn 2009/22/EG van het Europees Parlement en de Raad van 23 april 2009 betreffende het doen staken van inbreuken in het raam van de bescherming van de consumentenbelangen (PB L 110 van 1.5.2009, blz. 30).
[25] Zoals bijvoorbeeld: https://www.consumentenbond.nl/acties/facebook en https://www.parool.nl/amsterdam/uber-chauffeurs-beginnen-rechtszaak-over-privacyrechten~b2691fe8/.

categorieën met name van belang. Alleen schade die in causaal verband staat met de gebeurtenis waarop de schade berust, kan worden vergoed (artikel 6:98 Burgerlijk Wetboek).

Een benadeelde dient de aantasting van de eer of goede naam of van de persoon op andere wijze in uitgangspunt met concrete gegevens te onderbouwen. Uit rechtspraak van de Hoge Raad over aantasting van de persoon op andere wijze volgt dat een aantasting in sommige gevallen kan worden aangenomen, zonder dat een concrete onderbouwing nodig is. Dit kan het geval zijn als de aard en de ernst van de normschending meebrengen, dat de nadelige gevolgen daarvan voor de benadeelde voor de hand liggen (Hoge Raad, 15 maart 2019, ECLI:NL:HR:2019:376 en Hoge Raad, 19 juli 2019, ECLI:NL:HR:2019:1278). Een voorbeeld hiervan is het geval van de Oudejaarsrellen in Groningen uit 1997, waarin bewoners van een belaagd pand uren in angst en onzekerheid tevergeefs op politieondersteuning hadden gewacht (Hoge Raad, 9 juli 2004, ECLI:NL:HR:2004:AO7721). Dit is de uitzondering op de regel van de concrete onderbouwing, die alleen aan de orde is bij in het oog springende situaties. Uit voornoemde rechtspraak volgt ook dat van een aantasting in de persoon op andere wijze als bedoeld in art. 6:106 lid 1, onder b, BW, niet al aan orde is, bij de enkele schending van een fundamenteel recht. Het onzorgvuldig handelen alleen rechtvaardigt met andere woorden geen schadevergoeding. De schade van de benadeelde dient vast te staan.

Voor de begroting van de omvang van schade geldt dat concrete begroting het uitgangspunt is (artikel 6:97 Burgerlijk Wetboek). In recente rechtspraak overweegt de Hoge Raad dat de omvang van een verplichting tot vergoeding van schade die bestaat in een aantasting in de persoon op andere wijze (zie onder iii hiervoor), zich niet 'min of meer forfaitair' laat vaststellen. Dit is niet verenigbaar met het hoogst persoonlijke karakter van de vordering tot vergoeding van deze immateriële schade. Een rechter kan in een concrete zaak wel een bedrag vast stellen waaruit de schade van de benadeelden ten minste bestaat (Hoge Raad, 19 juli 2019, ECLI:NL:HR:2019:1278).

Bij een inbreuk op de AVG of een fundamenteel recht, strekt schadevergoeding alleen tot vergoeding van daadwerkelijk geleden schade, aldus de Afdeling Bestuursrechtspraak van de Raad van State.[26] Ook volgens vaste rechtspraak van het Hof van Justitie geldt dat te vergoeden schade reëel en zeker moet zijn (vergelijk het arrest van het Hof van Justitie van 4 april 2017, C- 337/15 P, Europese Ombudsman tegen Staelen, ECLI:EU:C:2017:256, punt 91).[27]

Uit voorgaande rechtspraak volgt dat een op zichzelf staande schending van een fundamenteel recht niet altijd leidt tot een schadevergoeding. Daarbij komt dat schade op grond van de wet in ieder individueel geval moet worden begroot. Het kabinet ziet dan ook geen aanleiding en ook geen mogelijkheid om voor zaken waarin big data aan de orde is vaste bedragen voor schadevergoeding vast te stellen. Big data kan in vele uiteenlopende situaties aan de orde zijn. Ook onrechtmatig handelen is in deze context niet in één vat te gieten. Schade en schadevergoedingen zijn dat daarom evenmin. Dit geldt eens te meer wanneer er sprake is van immateriële schade, omdat de gevolgen voor de individuele benadeelde maatgevend zijn voor de omvang van de schadevergoeding. Vaste bedragen leiden tot over- of ondercompensatie. Dit is niet te rechtvaardigen jegens individuele benadeelden en schadeveroorzakers. Dit neemt niet weg dat partijen in een concrete zaak afspraken kunnen maken over vaste bedragen, die recht doen aan de omstandigheden van het geval. Ook een rechter kan in een specifieke zaak een minimale schadevergoeding vast stellen. De WAMCA laat partijen en de rechter hiertoe de ruimte.

Op het alternatieve voorstel voor bekostiging van processen middels het instellen van een processenfonds zal worden ingegaan bij behandeling van reguleringsoptie XI.

[26] Zie: ECLI:NL:RVS:2020:899 (Deventer), overwegingen 21 tot en met 35.
[27] Zie: ECLI:NL:RVS:2020:899 (Deventer), overweging 22.

Reguleringsoptie V: maak duidelijk in welke gevallen (indirecte) discriminatie in big data toepassingen kan of moet leiden tot bewijsuitsluiting of strafvermindering

De onderzoekers kaarten hier aan dat het zo kan zijn dat een opsporingsinstantie een onderzoek instelt op basis van de uitkomst van een data-analyse, naar aanleiding waarvan er gericht wordt gepatrouilleerd of gezocht in bepaald onderdeel van de populatie (bijv. een postcodegebied). Indien vervolgens bewijs wordt gevonden tegen een individu uit deze populatie, zal dit individu worden voorgeleid aan de rechter. De strafrechter zal vervolgens oordelen dat het gevonden bewijs rechtmatig is, maar zal zich niet buigen over de oorspronkelijke analyse die leidde tot een bepaald deel van de bevolking. Dit terwijl daar bijvoorbeeld een bepaalde vooringenomenheid (*bias)* aan ten grondslag kan hebben gelegen. De onderzoekers opteren ervoor om een eventuele onrechtmatige ´voor analyse´ mee te laten wegen in het strafproces, bijvoorbeeld door bewijsuitsluiting of strafverminderingen het geval het bewijs is vergaard op basis van gebrekkige methoden.

In het rapport wordt al genoemd dat er via de bestuursrechtelijke weg mogelijkheden zijn om een eventuele onrechtmatige vooranalyse aan te vechten. Het kabinet ziet in dergelijke gevallen eerder aanleiding een zaak te starten bij de civiele rechter. Voorts staat natuurlijk ook een beroep op het gelijke behandelingsrecht of relevante mensenrechtenverdragen open. Voorliggende reguleringsoptie ziet dus specifiek op dat de strafrechter de vooranalyse niet meeneemt en beoordeelt; het is niet zo dat dergelijke analyses niet kunnen worden tegengaan.

Allereerst is belangrijk te benadrukken dat wanneer besloten wordt een individu aan te houden, maar dit niet leidt tot het aanspannen van een zaak bij de rechter, het individu schadevergoeding kan vorderen voor het strafvorderlijk optreden via de bepalingen in hoofdstuk 6 van het nieuwe wetboek van strafvordering. Als zou blijken dat de aanhouding (mede) was ingegeven door onrechtmatige data-analyse kan het individu, naast de schadevergoeding voor het strafvorderlijk optreden, zoals eerder vermeld ook een zaak bij de civiele rechter aanspannen bijvoorbeeld wegens onrechtmatig overheidshandelen.

Wanneer de aanhouding wel leidt tot een zaak bij de strafrechter, zal tevens aan de orde komen of het individu terecht als verdachte is aangemerkt. Als een vorm van data-analyse een rol heeft gespeeld in de redenering om iemand als ´verdachte´ aan te merken, of op andere wijze invloed heeft op de casus, zal de rechter indien nodig (en eventueel op verzoek van de advocaat van verdachte) ook toetsen of die analyse rechtmatig is. Dit betekent dat de rechter de vooranalyse weldegelijk zal toetsen. Het kabinet wil daarbij benadrukken dat van belang is te wegen wat de invloed van de analyse op de keuze van de opsporingsdiensten is geweest. Er kan immers niet worden gesteld dat, ook al heeft de vooranalyse niet bepaald wie wordt aangehouden maar opsporingsdiensten slechts een bepaalde kant op gestuurd, er geen relatie kan bestaan tussen de data-analyse en het besluit om aan te houden. Het feit dat opsporingsdienst een bepaalde kant op worden gestuurd kan bewust of onbewust meewegen in de individuele keuze van een opsporingsambtenaar om op een bepaalde wijze te handelen. Het is daarmee aan de rechter om per zaak te wegen wat de invloed van de vooranalyse is geweest op de keuze om verdachte aan te houden.

De reguleringsoptie is dus slechts relevant voor situaties waarin er een ´vooranalyse´ wordt gedaan waarin een bepaalde *bias* zit, maar vervolgens los daarvan, en niet op basis van die foutieve/onrechtmatige analyse, wordt besloten om de verdachte aan te houden. Het ligt wat het kabinet betreft niet voor de hand om, specifiek gelet op het gelijkheidsbeginsel, een rechtmatig aangehouden verdachte minder zwaar te straffen voor eenzelfde vergrijp. Wanneer er wél invloed is geweest op de gemaakte keuzes binnen het strafproces valt de data-analyse immers al binnen het toetsingskader van de strafrechter. Zoals de onderzoekers zelf ook al opmerken: het ligt niet direct voor de hand om gebreken in big-data toepassingen te verhelpen via het strafrecht.

Reguleringsoptie VI: breid de mogelijkheid tot participatie voor rechtspersonen in het strafrecht uit

Uit het onderzoek blijkt dat de rechtspersonen die in het algemeen belang procederen zich niet richten op het strafrecht, omdat de kans op succes laag wordt ingeschat en de rechtspersoon niet bepaalt welke (juridische) argumentatie wordt gevolgd. De rechtspersoon in kwestie is immers geen partij in een de strafrechtelijke procedure.

Om wél mogelijkheid daartoe te introduceren kan worden gekeken naar het Franse rechtssysteem waar het vervolgingsmonopolie in bepaalde gevallen ook aan rechtspersonen toe kan komen, bijvoorbeeld aan een vereniging die in het collectief belang vervolging in wil stellen.

Als minder verstrekkend alternatief leggen de onderzoekers voor dat de mogelijkheden voor voeging uitgebreid kunnen worden ten aanzien van de reeds bestaande mogelijkheid om te voegen teneinde schadevergoeding te vorderen uit artikel 51f Sv. Dit zou betekenen dat een organisatie zich zou kunnen voegen wanneer een big data toepassing leidt tot een ongewenst effect in het strafproces van een verdachte, om aan een rechter uit te leggen hoe dat big data proces werkt.

Ten aanzien van het minder verstrekkend alternatief merkt het kabinet op dat het vergroten van de mogelijkheid voor rechtspersonen om zich te voegen in het strafproces niet wenselijk. Allereerst is het zo dat de rechter de regie over het strafproces voert. Het is dan ook aan de rechter, eventueel op verzoek van de verdediging, om te bepalen of deskundigen worden betrokken om bijvoorbeeld een big-data toepassing te doorgronden. Op deze wijze kunnen organisaties dus toch een rol vervullen in het strafproces. Daarbij komt dat het strafproces een systeem kent waarin het aantal deelnemers in beginsel beperkt is. Indien partijen zich kunnen voegen kunnen zij op eigen initiatief invloed uitoefenen op dit afgebakende proces. Hierdoor zou de regie op het eigen proces van verdachte beperkt worden. Voorts kan het ook zo zijn dat rechtspersonen andere belangen hebben dan verdachte. Verdere mogelijkheden tot voegen kunnen dus negatieve consequenties hebben voor het eerlijk proces van een verdachte.

Deels ten overvloede gelet op bovenstaande passage over voeging door rechtspersonen in het strafproces, merkt het kabinet op dat de meer vergaande figuur uit het Franse recht niet wenselijk is. Deze figuur, waarbij het vervolgingsmonopolie wordt uitgebreid, zou een nog verdere inbreuk vormen op de regie op het eigen proces van de verdachte en op de autonomie van de rechter. Daarbij komt dat een dergelijke figuur niet past in het Nederlandse systeem, waarin het Openbaar Ministerie werkt met een positief opportuniteitsbeginsel. Het kabinet zal deze opties dan ook niet overnemen.

Het kabinet juicht het wel toe dat (rechts)personen hun expertise over big-data processen in willen zetten ter ondersteuning van het strafproces. Indien (rechts)personen hun expertise in het algemeen belang in willen zetten in rechtszaken, bijvoorbeeld door te toetsen of analyses onrechtmatig/onjuist zijn, wijst het kabinet hen op de mogelijkheid om een natuurlijk persoon te laten registreren in het Nederlands Register Gerechtelijk Deskundigen (artikel 51k Sv). Indien zij graag aan een specifieke zaak bij willen dragen kunnen zij dit vervolgens bij de advocaten van verdachte bekend maken. Deze kunnen de persoon in kwestie desgewenst als deskundige oproepen.

Reguleringsoptie VII: introduceer de Special Advocate

Deze reguleringsoptie geeft in overweging de figuur van de ´special advocate´ in het Nederlandse recht te introduceren. De onderzoekers beschrijven dat er soms de spanning ontstaat tussen het recht op informatie van een betrokkene (zoals vastgelegd in AVG en de Wet Politie Gegevens) en het gebruik van algoritmen in opsporing en onderzoek. De informatierechten van betrokkenen kunnen vervolgens in het belang van bijvoorbeeld nationale veiligheid en openbare orde worden

beperkt, omdat inzicht in de werking van algoritmische systemen voordeel op kan leveren voor kwaadwillenden.[28]

Deze spanning culmineert wanneer algoritmen een rol spelen in de opsporing en relevant zijn voor het strafdossier van de burger, maar verdachte geen toegang krijgt tot de informatie in kwestie. De onderzoekers wijzen daarbij onder meer op de commissie Koops[29] die in 2018 stelde dat de wetgever kan overwegen de momenteel impliciete eis van uitlegbaarheid van strafvorderlijke beslissingen te expliciteren indien deze beslissing (mede) op geautomatiseerde data-analyse wordt gebaseerd.

De onderzoekers stellen dat als de wetgever meer bescherming wil bieden op dit punt, overwogen kan worden om de ´special advocate´ te introduceren, een persoon of instantie die een verdachte verdedigt maar die niet is aangesteld door de verdachte en geen instructies van diegene ontvangt. Deze *special advocate* zou, onder uitzonderlijke omstandigheden wanneer er een absolute noodzaak is om de verdachte geen toegang te geven tot de onderliggende stukken, toegang kunnen krijgen tot de algoritmen en gegevens in kwestie. Er zou dan een orgaan moeten worden ingesteld om te bepalen of er inderdaad sprake is van een dergelijke uitzonderlijke situatie waarin verdachte geen inzicht kan krijgen in de stukken betreffende zijn eigen proces. De onderzoekers merken op dat de procesautonomie van de verdachte hiermee ingrijpend wordt beperkt, de *special advocate* kan immers niet met verdachte overleggen, noch kan de verdachte bepaalde feiten betwisten.

Het kabinet ziet net als de onderzoekers dat er een bepaalde spanning kan bestaan tussen de noodzaak voor de verdachte om inzicht te verkrijgen in gegevens en op basis daarvan acterende algoritmen, versus de beperkingen op de transparantie van bepaalde algoritmen in het belang van nationale veiligheid en onderzoek. Het is dan ook van belang om de gegevens en algoritmen in kwestie onafhankelijk te kunnen laten toetsen. Desalniettemin is het kabinet niet voornemens hiervoor de figuur van de *special advocate* te introduceren.

Allereerst is genoemde figuur, zoals de onderzoekers reeds opmerken, omstreden. Deze *special advocate* moet namelijk opkomen voor de belangen van verdachten , maar mag geen informatie uitwisselen met de verdachte. Het is onduidelijk hoe de *special advocate* kan weten wat het ´belang´ van verdachte is en hoe dit kan worden behartigd, wanneer geen informatie met verdachte mag worden uitgewisseld. Deze figuur zou daarmee inbreuk maken op de procesautonomie van verdachte, hetgeen het kabinet onwenselijk acht. Dit geldt te meer omdat er ook oplossingen bestaan waarbij dat niet het geval is.

Ten tweede ziet het kabinet namelijk dat het strafprocesrecht reeds voldoende mogelijkheid biedt om onafhankelijk onderzoek te laten verrichten naar gegevens of algoritmen die niet openbaar kunnen worden gemaakt. Indien de officier van justitie besluit om de voeging van bepaalde stukken achterwege te laten met oog op de in artikel 187d eerste lid Sv genoemde belangen behoeft hij daartoe een machtiging van de rechter-commissaris (Hierna: ¨RC¨). De RC kan op verzoek van de verdediging of deskundige onderzoek doen zonder het dossier openbaar te maken. De RC kan zich hierbij overigens ook weer bij laten staan door een deskundige uit het Nederlands Register Gerechtelijk Deskundigen.[30] Daarmee wordt geborgd dat alle partijen kunnen vragen om een onafhankelijke blik, ook op gegevens of analyses die niet openbaar kunnen worden gemaakt.

Voorts benoemen onderzoekers nog de mogelijkheid de *special advocate* ook in het bestuursrecht te introduceren. Deze zou dan bijvoorbeeld toetsen of informatie terecht door een rechter buiten de procedure is gehouden omdat er een gerechtvaardigd belang zou zijn voor één van de partijen,

[28] Aan deze balans tussen transparantie en beperkingen daarvan wordt door het kabinet aandacht besteed in reactie op de initiatiefnota Middendorp (Kamerstukken II, 2019/20, 35 212, nr. 3)
[29] Commissie modernisering opsporingsonderzoek in het digitale tijdperk (2018): ¨regulering van opsporingsbevoegdheden in een digitale omgeving.¨ p. 28.
[30] (Zie daarover ook onder reguleringsoptie VI).

zoals bedoeld in artikel 8:29 Awb. Het kabinet vindt het niet wenselijk een aparte entiteit in het leven te roepen die bepaalt of een rechter een toetsing juist uitvoert.

De door de onderzoekers genoemde mogelijkheid om de uitlegbaarheidseis bij data-analyse in het strafvorderingsproces expliciet te maken, wordt betrokken bij de modernisering van het Wetboek van Strafvordering.

Reguleringsoptie VIII: stelt beroepsmogelijkheden open tegen algemeen verbindende voorschriften en beleidsregels

De onderzoekers stellen dat het bestuursrecht in de toekomst belangrijker zal worden voor het adresseren van vraagstukken omtrent Big Data-processen. Wanneer er op basis van verzamelde en geanalyseerde data beleid en algemeen verbindende voorschriften worden ontwikkeld, zou het naar de mening van de onderzoekers wenselijk zijn als burgers en organisaties die hen vertegenwoordigen, daartegen beroep kunnen instellen indien zij van mening zijn dat deze zijn gebaseerd op bijvoorbeeld een onbetrouwbare database, een algoritme met een bias of een algoritme dat een impliciet stigmatiserende werking zou kunnen hebben. Daarom stellen zij voor om artikel 8:3 Awb, dat beroep tegen algemeen verbindende voorschriften en beleidsregels uitsluit, te wijzigen.

Met de onderzoekers is het kabinet van mening dat het recht op toegang tot de rechter en het recht op een effectief rechtsmiddel van wezenlijk belang zijn in een democratische rechtsstaat. Nieuwe technologieën, waaronder big data-analyses, worden in toenemende mate ingezet binnen de rechtspleging en het openbaar bestuur en deze ontwikkeling levert vragen op vanuit dit perspectief. Het kabinet ziet gelet op de in het rapport geschetste problematiek echter onvoldoende reden om over te gaan tot wijziging van artikel 8:3 Awb. Ten eerste leidt aanpassing van artikel 8:3 Awb niet tot vermindering van de in het rapport geïdentificeerde problematiek ten aanzien van het bestuursrecht omdat de problematiek omtrent de inzet van big data-processen zich hoofdzakelijk manifesteert ten aanzien van feitelijke handelingen en voorbereidingshandelingen. Ten tweede doen de argumenten die eerder zijn gegeven ter onderbouwing van de onwenselijkheid om over te gaan tot wijziging van artikel 8:3 Awb ook in het licht van de door de onderzoekers geschetste ontwikkeling, nog steeds opgeld (vgl. Kamerstukken II 29279, nr. 16, p. 12-13). Het kabinet verwacht allereerst een doorbreking van het evenwicht tussen bestuur en rechter als de mogelijkheden voor de rechter om regelgeving te toetsen worden verruimd. De controle op deze regelgeving dient in de eerste plaats toe te komen aan vertegenwoordigende lichamen als de Staten-Generaal, de provinciale staten en de gemeenteraad. Ten tweede verwacht het kabinet dat de voortgang van het bestuurshandelen wordt belemmerd door onzekerheid over de daadwerkelijke inwerkingtreding van de algemeen verbindende voorschriften en beleidsregels. Ten derde wijst het kabinet op de te verwachten toename van het aantal beroepen bij de rechter, in een tijd waarin de bestuursrechter toch al overbelast is. De bestuursrechtspraak is hier niet op berekend en de hiervoor benodigde budgetten zijn niet beschikbaar. Dit alles betekent dat het kabinet geen wetgeving in procedure zal brengen die strekt tot het laten vervallen van artikel 8:3, eerste lid, van de Awb.

Voorts zij opgemerkt dat de onderzoekers onder deze reguleringsoptie ook verwijzen naar het relativiteitsvereiste en het niet kunnen aantekenen van bezwaar en beroep tegen feitelijke handelingen. Wat betreft de verwijzing naar het relativiteitsvereiste deelt het kabinet de observatie dat Big Data processen vaak geen direct effect hebben op specifieke burgers. Indien op basis van big-dataprocessen besluitvorming jegens specifieke burgers plaatsvindt, kunnen zij tegen dergelijke besluiten opkomen. In dat kader is toepassing van artikel 8:69a Awb niet problematisch. Wat betreft de tweede opmerking over het niet kunnen aantekenen van beroep en bezwaar tegen feitelijke handelingen begrijpt het kabinet waarom de onderzoekers deze problematiek aandragen. Zoals hierboven ten aanzien van het voorstel om artikel 8:3 Awb te schrappen benoemd ziet het kabinet dat problematiek omtrent big-data processen zich vooral

manifesteert omtrent feitelijke- en voorbereidingshandelingen. Tegen dergelijke handelingen staat thans beroep open bij de civiele rechter. De rechtsbescherming is hier derhalve niet in het geding. Overigens onderzoekt het kabinet of verruiming van de bevoegdheid van de bestuursrechter tot feitelijke handelingen in het kader van de integrale geschilbeslechting in het sociaal domein wenselijk is.[31] Als laatste verdient opmerking dat het kabinet de geconstateerde relevantie van algoritmen die geen ´awb-besluit´ nemen maar wel een bepalende rol spelen bij een besluitvormingsproces ook door laat klinken in haar reeds ingezette beleid. Bij de verdere doorontwikkeling van de eerder genoemde ´richtlijnen voor data-analyse door de overheid´ wordt meegenomen dat de ´impact´ van een algoritme niet alleen moet worden bezien aan de hand van het effect van het uiteindelijke besluit op de burger, maar ook in het licht van de rol die het algoritme speelt in de totstandkoming van de besluitvorming. Daarmee worden ook algoritmen die géén direct besluit nemen onder de reikwijdte van de richtlijnen gebracht.

Reguleringsoptie IX: breid de mogelijkheden rond het stellen van prejudiciële vragen uit

De onderzoekers leggen deze reguleringsoptie voor als één van de mogelijkheden om de kosten van collectieve acties terug te dringen. Geïnterviewde collectieve belangenorganisaties hebben aangegeven dat zij om de kosten van een proces te beperken strategisch aansturen op prejudiciële vragen, zodat in eerste aanleg toch al een uitspraak van de hoogste rechter kan worden verkregen.

Er wordt in het rapport benoemd dat er binnen Nederland een goed werkend stelsel bestaat voor het stellen van prejudiciële vragen. Artikel 392 Rv stelt de civiele rechter in de gelegenheid om op verzoek van een partij of ambtshalve de Hoge Raad een rechtsvraag te stellen indien deze vraag: nodig is om op de eis of het verzoek te beslissen én rechtstreeks van belang is voor een veelheid van vorderingsrechten die gegrond zijn op dezelfde feiten of voortvloeien uit soortgelijke samenhangen oorzaken, óf voor de beslechting of beëindiging van talrijke andere uit soortgelijke feiten voortvloeiende geschillen waarin dezelfde vraag zich voordoet. Daarnaast zijn er ook mogelijkheden voor rechters om vragen voor te leggen aan het Europese Hof van Justitie, en voor de Hoge Raad om vragen voor te leggen aan het Europese Hof voor de Rechten van de Mens.

Daarnaast wijzen de onderzoekers erop dat de mogelijkheid tot het stellen van prejudiciële vragen ook in boek 6 van het nieuwe Wetboek van Strafvordering is opgenomen, met het voornemen deze mogelijkheid via een Innovatiewet Strafvordering vanaf 2021 in experimentvorm op te stellen. De Innovatiewet Sv ligt momenteel voor advies bij de Raad van State, dit advies wordt medio oktober verwacht. Het is van belang daarbij op te merken dat deze bepaling ook een afgebakende mogelijkheid biedt voor het stellen van prejudiciële vragen. Hier worden drie voorwaarden verbonden: allereerst moet het antwoord op de vraag nodig zijn om in de zaak te beslissen, ten tweede moet aan beantwoording van die vraag bijzonder gewicht worden toegekend en ten derde moet er sprake zijn van ´zaak overstijgend belang´.

Onderzoekers leggen twee manieren voor waarop de bestaande regeling voor het stellen van prejudiciële vragen verder uitgebreid kan worden in aanvulling op bovengenoemde regelingen in het civiel- en strafrecht.

Ten eerste door de mogelijkheid voor het stellen van prejudiciële vragen ook in het bestuursrecht te introduceren. Het kabinet wijst erop dat waar spoed noodzakelijk is, er reeds mogelijkheid in het bestuursrecht bestaat toch rechtspraak in één instantie. Dit maakt het proces wezenlijk anders dan in het strafproces en civiele recht, waar procedures langer kunnen duren. Het ligt dan ook niet voor de hand de mogelijkheid tot het stellen van prejudiciële vragen te verbreden in het bestuursrecht. Daarbij komt dat het in veel gevallen hoogst waarschijnlijk sneller zal zijn om een uitspraak van de rechtbank te verkrijgen en vervolgens desgewenst in beroep te gaan.

[31] Kamerstukken II, 2019/20, 34 477, nr. 69.

Ten tweede door de mogelijkheid tot het stellen van prejudiciële vragen in de Nederlandse rechtsorde niet alleen open te stellen voor rechtsvragen die ook in veel andere zaken spelen, maar ook voor zaken die worden gevoerd in het ´algemeen belang´. De huidige benadering werkt vooral voor zaken in het collectief belang en bij het afdoen van massaclaims, maar rechtsvragen in algemeen belang acties zijn niet altijd relevant voor een veelheid aan rechtszaken.

Het kabinet ziet geen aanleiding om de mogelijkheid tot het stellen van prejudiciële vragen in het civiele- en strafrecht te verruimen. De prejudiciële procedure kent namelijk ook nadelen. In het individuele geval leidt de procedure bijvoorbeeld tot vertraging, waardoor betrokkenen langere tijd in onzekerheid blijven. Voorts heeft het feit dat het lopende proces wordt aangehouden, organisatorisch gevolgen: op basis van de agenda's van procespartijen, getuigen en de rechtbanken moeten nieuwe zittingsdata worden gepland en betrokkenen worden opgeroepen. Verder wordt beslag gelegd op de schaarse capaciteit van de Hoge Raad. In het civiele recht en het strafrecht wegen deze nadelen op tegen de voordelen, juist doordat een antwoord van de Hoge Raad betekenis heeft voor (veel) andere zaken. Deze (andere) zaken kunnen sneller worden opgelost. Dat is de kern van de toegevoegde waarde van de prejudiciële procedure. Deze toegevoegde waarde ontbreekt bij zaken die in het algemeen belang worden gevoerd, terwijl er wel voldoende alternatieven zijn om relatief snel dergelijke vragen te beantwoorden. Partijen kunnen bijvoorbeeld in civiele zaken overeenkomen een feitelijke instantie over te slaan of hun zaak meteen aan het Hof ter beoordeling voorleggen.[32] Ook kunnen partijen vragen om snellere behandeling van hun zaak.

Reguleringsoptie X: breid de mogelijkheden van *amicus curiae* participatie uit

Deze reguleringsoptie legt voor om de *amicus curiae* figuur toe te voegen aan het Nederlands rechtsbestel. In dat geval kunnen partijen zich als ´vriend van het Hof´ uitspreken over aan de zaak gerelateerde vraagstukken. Artikel 8:45a Awb stelt reeds een vergelijkbare figuur open voor de Europese Commissie en de Autoriteit Consument en Markt. Achtergrond van het voorleggen van deze figuur is wederom het beperken van de kosten van een proces voor rechtspersonen.

De onderzoekers stellen voor om de mogelijkheden voor *amicus curiae* participatie uit te breiden naar het strafrecht en het civiele recht. Ten tweede opteren ze om de figuur meer in te zetten in zaken die worden gevoerd in het algemeen belang. In genoemd rapport over de *amicus curiae* bij de RvS gaven geïnterviewden aan dat de inzet daarvan minder voor de hand ligt in politiek en maatschappelijk sensitieve zaken. Dit terwijl het bij algemeen belang zaken over big data processen vaak lastig is om te duiden wat de concrete gevolgen zijn van een big data proces. Hulp van een gespecialiseerde rechtspersoon kan dan ook van groot nut zijn volgens de onderzoekers.

Het kabinet wijst erop dat recent een wetsvoorstel bij de Tweede Kamer is ingediend waarin wordt voorgesteld om de figuur van de *amicus curiae* in procedures bij de hoogste bestuursrechters wettelijk te verankeren (Kamerstukken II 2019/20, 35 550, nr. 1-2). Deze figuur houdt kort gezegd in dat ook anderen dan de bij een rechtzaak betrokken partijen de gelegenheid kunnen krijgen om in die zaak een inbreng te leveren (mee te denken). "Meedenkers" kunnen door hun inbreng in een procedure voor de rechter een bijdrage leveren aan de rechtsontwikkeling. Door de inbreng van anderen dan partijen kan de rechter een beter, breder zicht krijgen op de mogelijke maatschappelijke gevolgen van een te nemen beslissing.

Het voorstel om een *amicus curiae* in te voeren in het civiele recht uit oogpunt van kostenbesparing neemt het kabinet niet over. Anders dan de onderzoekers verwacht het kabinet dat toevoeging van een *amicus curiae niet* per se leidt tot een daling van de kosten van de procedure. Het toevoegen van een extra betrokkene aan de procedure betekent dat partijen niet langer alleen op elkaar moeten reageren, maar ook hetgeen de *amicus curiae* naar voren brengt in

[32] Zie boek 1 titel 6 Wetboek van Burgerlijke Rechtsvordering.

de procedure. Dit kan de procedure compliceren en vertragen. Als partijen het niet eens zijn met de *amicus curiae* kan het weerleggen van diens advies bovendien nader (kostbaar) onderzoek vergen. Het civiele procesrecht biedt daarnaast andere mogelijkheden om voldoende relevante informatie in de procedure te krijgen. Op verzoek van partijen of ambtshalve kan de rechter een deskundigenonderzoek laten uitvoeren en de kosten daarvan voorlopig laten betalen door de partij die hiervoor het meest in aanmerking komt. Daarnaast verduidelijkt het wetsvoorstel vereenvoudiging en modernisering bewijsrecht, dat op dit moment bij Uw Kamer aanhangig is,[33] de mogelijkheden om relevante informatie te verkrijgen van de wederpartij of een derde. Daarmee zijn er volgens het kabinet voldoende mogelijkheden om, ook in zaken over big data, alle relevante informatie in de procedure te krijgen.

De argumenten ten aanzien van de kosten en lengte van de procedure en het deskundigenonderzoek in het civiele recht, gelden net zo goed ten aanzien van de mogelijkheid om de *amicus curiae* uit te breiden naar het strafrecht. Daar komt bij dat de voorgestelde figuur wat het kabinet betreft ook om meer principiële reden niet in het strafrecht thuishoort. Het zou niet passen bij de regie die strafrechter over een zaak voert. Het zou dan ook onwenselijk zijn indien een *amicus curiae* zich uitspreekt over een nog lopend proces.

Reguleringsoptie XI: creëer een processenfonds voor de Big Data Context

De onderzoekers benadrukken bij meerdere reguleringsopties dat een groot obstakel voor rechtspersonen die in het collectief of algemeen belang willen procederen bestaat in het bijeen krijgen van de noodzakelijke financiële middelen voor het voeren van het proces. Deze rechtspersonen bestaan vaak op basis van *ad hoc* financiering en zijn daarmee niet snel geneigd zich te committeren aan langlopende zaken. Dit is des te meer het geval wanneer het een rechtszaak in het algemeen belang betreft, aangezien daar minder concreet zicht is op een eventuele schadevergoeding.

Teneinde te borgen dat belangrijke zaken in het collectief of algemeen belang niet vroegtijdig sneuvelen wegens een gebrek aan financiële middelen, of aan zekerheid over toekomstige middelen, stellen de onderzoekers voor een ´processenfonds´ in het leven te roepen voor rechtszaken in de big-data context. Een onafhankelijke stichting zal dit fonds beheren en bepalen welke aanvragen voor financiële middelen worden gehonoreerd.

Een dergelijk fonds kan worden gefinancierd door vanuit de overheid jaarlijks een bedrag aan het fonds toe te kennen, of door te kiezen voor een eenmalige donatie waarna de stichting inkomsten moet genereren uit schadevergoedingen die worden toegekend in gefinancierde zaken. Deze tweede vorm leent zich minder voor zaken in het algemeen belang, nu daaruit vaak minder of geen toekenning van schadevergoeding voortvloeit. Dit kan ertoe resulteren dat de stichting alleen zaken kan financieren met een grote kans op uitbetaling van schadevergoeding.

Zoals onder reguleringsoptie IV aan de orde is gekomen heeft het kabinet de mogelijkheden voor het voeren van collectieve acties de afgelopen jaren verruimd. Het is daarbij van groot belang om te borgen dat burgers daadwerkelijk van deze mogelijkheden gebruik kunnen maken. Het financieren van collectieve zaken kan in de praktijk lastig zijn omdat er van tevoren geen zekerheid bestaat over een eventuele vergoeding van geleden schade om de proceskosten uit te financieren. Genoemde problematiek met betrekking tot de financiering van zaken lijkt ten grondslag te liggen aan, of op zijn minst op de achtergrond van invloed te zijn op, meerdere voorgestelde reguleringsopties in het onderzoek. Het kabinet heeft dan ook de indruk dat zowel het borgen van de toegang tot het recht, als wel het verruimen van de mogelijkheden voor collectieve entiteiten om zaken aan te brengen, vooral toeziet op het realiseren van voldoende financiering en in mindere mate op het aanpassen van het procesrecht. Het ziet dan ook waarom

[33] Kamerstukken II 2019/20, 35 49.

de onderzoekers voorstellen om een processenfonds in te richten. Het zal daarom onderzoek laten verrichten naar de noodzaak, kosten en vormgeving van een revolverend processenfonds. Dit onderzoek wordt niet beperkt tot een processenfonds specifiek voor de ´big data context´, maar zal ook andere (rechts)gebieden in acht nemen.

Reguleringsoptie XII: breid de mogelijkheden van handhavingsorganisaties en controlemechanismen uit

In het rapport wordt meermaals benoemd dat goed toezicht op algoritmen en algoritmische besluitvorming van groot belang is. Er wordt gesteld dat de Autoriteit Persoonsgegevens in beginsel goed is toegerust om hier op toe te zien. De AP houdt immers al toezicht op veel algoritmische besluitvorming, omdat daarbij persoonsgegevens worden verwerkt.

Inzake het toezicht op algoritmen en algoritmische besluitvorming wijst het kabinet op de kabinetsreactie op het onderzoek naar toezicht op overheidsalgoritmen.[34] Daarin heeft het kabinet reeds toegelicht hoe het toezicht op algoritmen in gebruik bij de overheid de komende jaren verder vorm moet krijgen. Dit omvat mede dat de integraliteit van het toezicht doorlopend zal worden geëvalueerd. Het toezicht op overheidsorganisaties is daarmee reeds voldoende in beeld gebracht. Het kabinet zal bij de ontwikkeling van de onderzoeksagenda ´normering en toezicht algoritmen´ meenemen of het toezicht op (algoritmische) data-analyse in de private sector ook in voldoende samenhang is belegd. Uw kamer wordt in december dit jaar nog geïnformeerd over deze onderzoeksagenda.[35]

Wat betreft de toekenning van middelen aan de AP wijst het kabinet op het (lopende) onderzoek van naar het budget van de AP dat momenteel wordt uitgevoerd. KPMG voert in opdracht van de AP en het ministerie van JenV een onderzoek uit naar de grondslagen van de financiering van de AP, de omvang van het budget en de risico's behorende bij verschillende scenario's. De resultaten van dit onderzoek worden in het najaar van 2020 verwacht.

Voorts stellen de onderzoekers voor om big data processen binnen de overheid vooraf te laten toetsen door een onafhankelijke commissie die als centraal punt binnen de overheid zou moeten fungeren. Deze externe commissie zou ieder project ook om de zoveel tijd door kunnen lichten om te kijken of beoogde doelen zijn behaald, daarmee aansluitend bij de onder reguleringsoptie III voorgestelde horizonbepaling. Het kabinet ziet naar aanleiding van het onderzoek naar toezicht op overheidsalgoritmen geen aanleiding om een dergelijke commissie in te stellen. Wél zet het kabinet in op een uitbreiding van de bestaande DPIA-verplichtingen door een algoritme impact assessment te ontwikkelen (zie reguleringsoptie II). Dit kan worden gekoppeld aan voorafgaande raadpleging bij de toezichthouders en aan een mogelijke publicatieverplichting.[36] Hiermee worden voldoende externe adviseurs betrokken bij de toetsing van algoritmen in gebruik bij de overheid.

Als laatste stellen de onderzoekers voor om een grotere rol toe te kennen aan meer specialistische ombudsmannen. Deze kunnen zowel onderzoeken uitvoeren, als bewustwording vergroten en voorlichting geven. De ombudsman zou ook een rol als mediator aan kunnen nemen, bijvoorbeeld tussen de overheid en de burger. De regering zou de rol van ombudsmannen in Nederland groter kunnen maken, specifiek door introductie van een speciale ombudsman voor Big Data processen. Het kabinet is niet voornemens om voor dit onderwerp een speciale ombudsman in het leven te roepen. De nationale ombudsman heeft reeds speciale aandacht voor dit thema en werkt aan een visie op het behoorlijk gebruik van data en algoritmen door de overheid. Daarbij staat hij in nauw

[34] Kamerstukken II, 2019/20, 35212, nr. 3 (bijlage 2).
[35] Brief ´ambtelijke projectgroep normering en toezicht algoritmen´ (wordt z.s.m. naar de TK verzonden).
[36] Kabinetsbrief initiatiefnota Middendorp ¨menselijke grip op algoritmen¨, pp. 9-10.

contact met onder meer de Algemene Rekenkamer en de Raad van State.[37]

Reguleringsoptie XIII: constitutioneel toetsingsverbod

De onderzoekers wijzen op het constitutioneel toetsingsverbod dat in de Nederlandse Grondwet is vervat. Zij wijzen erop dat het Europese Hof voor de Rechten van de Mens (EHRM) de laatste jaren *in abstracto* wetgeving beoordeelt op rechtmatigheid, rechtsstatelijkheid en legitimiteit. Het Hof toetst in die gevallen dus niet of een individu of groep concrete schade heeft geleden. Het Hof staat daarbij ook klachten toe van rechtspersonen die conform hun statuten opkomen voor het algemeen belang. Zij hoeven dan ook geen actuele of mogelijk toekomstige schade aan te tonen. De onderzoekers stellen voor de mogelijkheden voor *in abstracto* toetsing ook binnen Nederland in te voeren. Het kabinet benadrukt dat dit onderdeel is van een in Nederland lang lopende discussie.

Het kabinet heeft in de vervolgbrief op het Kabinetsstandpunt over het advies van de Staatscommissie parlementair stelsel om in Nederland constitutionele toetsing door de rechter mogelijk te maken aan de Tweede en Eerste Kamer meegedeeld aan dat advies geen gevolg te geven en daaromtrent geen voorstellen te doen.[38]

In aanvulling daarop merkt het kabinet op dat de constatering van de onderzoekers dat het EHRM in toenemende mate een abstractie toetsing verricht van wetgeving voor nuancering vatbaar is. Uitgangspunt onder het klachtrecht bij EVRM is nog steeds het vereiste van 'slachtofferschap', waardoor de klager(s) tenminste duidelijk moeten maken op welke wijze beweerdelijk een inbreuk is gemaakt op hun fundamentele rechten. Dat kan ertoe leiden dat een specifieke toepassing (in hun geval) tot dat resultaat leidt, maar het kan ook zo zijn dat dit onder veel meer omstandigheden het geval is, doordat aan de wet gebreken kleven die hoe dan ook tot een inbreuk leiden of kunnen leiden. Daardoor krijgt de beoordeling het karakter van een abstracte toets waar die in aanleg was begonnen als een concrete toets.

Het EHRM vereist dat de bepalingen van het EVRM een 'nuttig effect' sorteren en dat kan, onder omstandigheden, betekenen dat ook de nationale rechter bij toetsing aan het EVRM constateert dat welke toepassing van de wettelijke bepaling(en) dan ook geen met het EVRM verenigbaar resultaat oplevert. Dat is een vorm van 'abstracte toetsing' die in Nederland onder art. 94 GW ook wel kan voorkomen, maar geen algemene regel is.

Voorts wijst het kabinet erop dat dat constitutionele toetsing niet alleen door de rechter kan of moet worden verricht. Wetsvoorstellen kunnen in consultatie worden gebracht, wat met name bij internetconsultatie aan iedereen de mogelijkheid geeft om mogelijke bezwaren in te brengen tegen conceptwetsvoorstellen. Het aspect van de grondwettigheid van wetten is daarbij sinds deze zomer een afzonderlijk, maar uitdrukkelijk benoemd aspect. Het staat de genoemde belangenbehartigers volledig vrij om hun bezwaren tegen voorgenomen wetgeving in dit stadium naar voren te brengen.

Een ander aspect van belang, waar ook de Staatsommissie op heeft gewezen, is de constitutionele toetsing van wetgeving vooraf (ex ante) tijdens het wetgevingsproces. In de ambtelijke voorbereiding (naast de al genoemde internetconsultatie) bestaat aandacht voor constitutionele aspecten. Daarnaast is de Afdeling advisering RvS in het bijzonder gespitst op constitutionele aspecten van de wetgeving die ter advisering voorligt, evenals de Eerste Kamer die vooral let op aspecten van rechtsstatelijkheid en constitutionaliteit.

[37] https://www.nationaleombudsman.nl/nieuws/2020/ombudsman-werkt-aan-visie-op-behoorlijk-gebruik-van-data-en-algoritmen-door-de-overheid.
[38] Kamerstuk, 2019/20, 34430 nr. T.