Algoritmes en grondrechten

M.J. Vetzo, J.H. Gerards en R. Nehmelman

Boomjuridisch

De opkomst van algoritme-gedreven technologieën als Big Data, Internet of Things en Kunstmatige Intelligentie levert een breed scala aan nieuwe grondrechtelijke uitdagingen op. Deze technologieën hebben bijvoorbeeld effect op de keuzes die we maken en daarmee op onze persoonlijke autonomie, en ingebouwde vooroordelen in algoritmes kunnen leiden tot ongelijke behandeling.

Nadere identificatie en analyse van de diverse grondrechtelijke uitdagingen is nodig om een gerichte aanpak van de problemen mogelijk te maken. In dit boek wordt daarom, specifiek voor Nederland, in kaart gebracht wat de (potentiële) impact is van Big Data, het Internet of Things en Kunstmatige Intelligentie op vrijheidsrechten, gelijkheidsrechten, privacyrechten en procedurele rechten. Centraal staat de gemeenschappelijke deler van de drie algoritme-gedreven technologieën: het gebruik van slimme algoritmes.

Het boek biedt zo een actueel en systematisch overzicht van grondrechtelijke knelpunten in relatie tot een van de meest urgente maatschappelijke uitdagingen van dit moment. Dit maakt het boek relevant voor iedereen die zich vanuit juridisch of technologisch perspectief bezighoudt met digitalisering en recht, zowel in de wetenschap als in de (rechts)praktijk.

MONTAIGNE CENTRUM
VOOR RECHTSSTAAT EN RECHTSPLEGING

Dit is een publicatie in de reeks van het Montaigne Centrum voor Rechtsstaat en Rechtspleging, Universiteit Utrecht.

ISBN 978-94-6290-541-2

Boomjuridisch

Algoritmes en grondrechten

Algoritmes en grondrechten

Max Vetzo
Janneke Gerards
Remco Nehmelman

Boom juridisch
Den Haag
2018

Omslagontwerp: Textcetera, Den Haag
Opmaak binnenwerk: Ambrac, Deventer

Het onderzoek voor dit boek is uitgevoerd in het kader van het Montaigne Centrum voor Rechtsstaat en Rechtspleging en de Master Legal Research van de Universiteit Utrecht. De uitgave is mede tot stand gekomen door een bijdrage van de Directie Constitutionele Zaken en Wetgeving van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties.

ISBN 978-94-6290-541-2
ISBN 978-94-6274-922-1 (e-book)
NUR 820

www.boomjuridisch.nl

INHOUDSOPGAVE

Inleiding

Aanleiding en onderwerp onderzoek

In diverse rapporten is reeds gewezen op nadelige effecten die digitalisering kan hebben op de bescherming van grondrechten.[1] Met het voortschrijden van technologische ontwikkelingen in de vorm van algoritme-gedreven technologieën als Big Data, het Internet of Things (IoT) en Kunstmatige Intelligentie (KI) doemen bovendien potentiële nieuwe grondrechtelijke knelpunten op. Op dit moment ontbreekt echter een specifiek op Nederland gerichte, juridische en systematische studie waarin wordt gereflecteerd op aantasting van grondrechtelijke bescherming als gevolg van deze technologieën en waarin wordt gekeken naar de effecten voor andere grondrechten dan informationele privacy en gegevensbescherming. Het onderhavige onderzoek, uitgevoerd in opdracht van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, beoogt dit hiaat te vullen.

Het rapport bestaat uit een 'quick-scan' waarin de (potentiële) impact wordt beschreven die Big Data, het IoT en KI op grondrechten in Nederland kan hebben. In het onderzoek wordt per technologische toepassing beschreven hoe deze werkt en op welke wijze(n) te verwachten valt dat de werking van die toepassing effecten heeft voor de uitoefening van een grondrecht. Daarbij wordt centrale aandacht besteed aan de grondrechtelijke implicaties van de gemeenschappelijke deler van deze technologieën: het gebruik van slimme algoritmes.

Het voorgaande leidt, conform de door het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties geformuleerde onderzoeksopdracht, tot de volgende onderzoeksvraag:

> *'Op welke wijze worden grondrechten in Nederland (mogelijk) aangetast als gevolg van het gebruik van Big Data, het Internet of Things en Kunstmatige intelligentie?'*

Methoden en aanpak

De in deze studie gehanteerde methode is die van 'klassiek' juridisch-dogmatisch onderzoek. Het betreft een bureaustudie op basis van Nederlandstalige en Engelstalige juridisch-wetenschappelijke literatuur, jurisprudentie van het Europees Hof voor de Rechten van de Mens en het Hof van Justitie van de Europese Unie alsmede Nederlandse rechtspraak,

1 Zie het rapport van de Commissie grondrechten in het digitale tijdperk 1999, Staatscommissie Grondwet 2010 en recenter WRR 2016, Kool e.a. 2017 en Van Est en Gerritsen 2017.

hier en daar aangevuld met rechtspraak van internationale semi-rechterlijke instanties als het VN-Mensenrechtencomité. Hierbij moet worden aangetekend dat het onderzoek in zoverre 'interdisciplinair' van karakter is, dat het geven van een overzicht van de relevante digitaliseringstrends (Big Data, IoT en KI) een noodzakelijk onderdeel vormt van de studie. Ten behoeve van het maken van deze 'review' is geput uit informatietechnologische artikelen, al dan niet in combinatie met (rechts)wetenschappelijke literatuur en overheidsrapporten waarin de informatie uit deze artikelen wordt besproken.

Het eigenlijke onderzoek naar de effecten van de genoemde drie technologische ontwikkelingen bestaat uit een 'quick scan'. Daarmee is de studie inventariserend van aard en noodzakelijkerwijs niet uitputtend. Dit maakt dat de beschrijving van de relevante technologieën zich beperkt tot de hoofdlijnen en zich richt op concrete toepassingen van Big Data, IoT en KI. Hetzelfde geldt voor de beschrijving van het grondrechtelijk kader. De kern van het rapport is gelegen in een analyse van de mogelijke consequenties van de drie algoritme-gedreven technologieën voor de genoemde clusters van grondrechten. Daarbij is noodzakelijkerwijs af en toe sprake van het weergeven van verwachtingen en veronderstellingen – op veel terreinen zijn de precieze gevolgen van de technologische ontwikkelingen nog moeilijk te voorspellen.

Afbakening

Het onderzoek is op vier manieren afgebakend:

1) Het onderzoek beperkt zich tot de genoemde drie, samenhangende technologieën: Big Data, IoT en KI. Specifieke toepassingen van deze technologieën door zowel de overheid als private partijen worden nader uitgewerkt en geïllustreerd met casuïstiek. Dit rapport beoogt geen uitputtend, diepgravend technologisch overzicht te geven van de drie technologieën en hun werking. In de beschrijving van de technologieën wordt voorgesorteerd op mogelijke grondrechtelijke knelpunten.
2) Het onderzoek beperkt zich tot de volgende clusters van grondrechten:

a) privacyrechten: het recht op privéleven, persoonlijke autonomie en menselijke waardigheid, aangevuld met het 'forum internum' (het hebben van een overtuiging en het koesteren van een mening);
b) gelijkheidsrechten: het recht op gelijke behandeling en non-discriminatie;
c) vrijheidsrechten: het recht op vrijheid van meningsuiting, vrijheid om informatie te ontvangen, de religieuze uitingsvrijheid ('forum externum'), vrijheid van betoging en vergadering en het kiesrecht;
d) procedurele rechten: het recht op een eerlijk proces en een effectief rechtsmiddel.

Het recht op persoonsgegevensbescherming wordt buiten beschouwing gelaten, omdat hier reeds veel en uitgebreid onderzoek naar is gedaan. Ook sociale grondrechten zijn niet in het onderzoek betrokken.

3) Het woord 'aangetast' in de onderzoeksvraag impliceert dat gezocht wordt naar mogelijke knelpunten in de grondrechtenbescherming of beperkingen van het effectieve genot van grondrechten, die (mogelijk) worden veroorzaakt door de toepassing van Big Data, IoT en KI. De invalshoek van het onderzoek is daarmee dat primair wordt gereflecteerd op grondrechtelijke uitdagingen ten gevolge van digitalisering. Kansen die voornoemde technieken bieden voor het effectueren van grondrechten worden soms kort aangestipt.
4) Uit het voorgaande volgt dat het onderzoek een specifiek juridisch karakter heeft, al is, zoals al aangegeven, ook geput uit de informatietechnologische literatuur om te kunnen voorzien in een overzicht van de werking van de relevante technologieën.

Opzet

Hoofdstuk I verschaft een overzicht van het functioneren van de drie technologieën die in het onderzoek centraal staan: Big Data, IoT en KI. Allereerst wordt in een korte eerste paragraaf een introductie gegeven op het begrip digitalisering en de drie specifieke technologieën die in het onderzoek centraal staan. Vervolgens worden in paragraaf I.2, I.3 en I.4 de drie technologieën apart behandeld; daarbij wordt een algemene beschrijving steeds gecombineerd met een bespreking van een aantal specifieke, voor het onderzoek mogelijk relevante toepassingen. In paragraaf I.5 wordt ingegaan op de gemeenschappelijke deler van de drie technologieën: het gebruik van slimme algoritmes.

In Hoofdstuk II wordt het grondrechtelijk kader geschetst. In iedere paragraaf wordt een cluster van grondrechten nader uiteengezet, aan de hand van de drie belangrijkste bronnen van deze grondrechten: de Grondwet, het Europees Verdrag voor de Rechten van de Mens en het Handvest voor de Grondrechten van de Europese Unie; sporadisch en waar relevant wordt ook de internationale grondrechtenbescherming in het overzicht betrokken. In paragraaf II.1 worden privacyrechten besproken, paragraaf II.2 richt zich op gelijkheidsrechten, paragraaf II.3 gaat in op vrijheidsrechten en paragraaf II.4 behandelt de procedurele rechten. In iedere paragraaf wordt ingegaan op onderwerpen als rationale, reikwijdte, concrete manifestaties en waar nodig op relevante leerstukken als positieve verplichtingen en horizontale werking. Ook hier is het niet het doel om uitputtend te zijn, maar vooral om een basis te creëren voor het begrijpen van de mogelijke problemen die zich binnen de reikwijdte van het betreffende grondrecht voor kunnen doen met betrekking tot algoritme-gedreven technologieën.

Hoofdstuk III vormt de kern van het onderzoek. In dit hoofdstuk worden de inzichten uit hoofdstukken I en II samengebracht en wordt bezien waar zich mogelijke knelpunten bevinden als gevolg van het gebruik van de algoritme-gedreven technologieën Big Data, IoT en KI. Per cluster van grondrechten wordt onderzocht of digitalisering (mogelijk) een negatieve impact kan hebben op de uitoefening van de betreffende grondrechten. Waar mogelijk en nodig wordt specifiek besproken welke technologische toepassing op welke manier tot problemen leidt of kan leiden voor wat betreft grondrechtelijke bescherming.

In Hoofdstuk IV worden de bevindingen uit hoofdstuk III samengevat en in samenhang bezien. Daarbij wordt eveneens een aanzet gegeven voor de beantwoording van de vraag waar zich de voornaamste grondrechtelijke knelpunten voordoen.

I Big Data, Internet of Things en Kunstmatige Intelligentie

I.1 Inleiding

In 2017 beschreef het Rathenau Instituut hoe de razendsnelle ontwikkeling en samenkomst van een veelheid aan technologieën heeft geleid tot een nieuwe fase in de digitale samenleving.[2] In deze fase zijn de fysieke en digitale wereld onlosmakelijk met elkaar verbonden en worden veel belangrijke beslissingen niet langer door mensen, maar door computers genomen. Big Data, het Internet of Things en Kunstmatige Intelligentie zijn belangrijke drijvers van dit proces van digitalisering. Deze drie technologieën kunnen het functioneren van overheden, bedrijven en het dagelijks leven van vele mensen aanzienlijk beïnvloeden.

De drie technologieën vertonen een grote mate van samenhang. Het Internet of Things (IoT) ziet op de ontwikkeling waarbij steeds meer 'alledaagse' apparaten met het Internet verbonden raken. Dergelijke apparaten kunnen data waarnemen en doorgeven en dragen zo bij aan een vergaande digitalisering van de fysieke wereld. Deze digitalisering heeft een enorme toename van data tot gevolg. Overheden en bedrijven zijn steeds beter in staat om relevante informatie uit grote hoeveelheden aan gevarieerde, veelal *real-time* data te destilleren en deze informatie te gebruiken ten behoeve van (automatische) besluitvorming. Dit wordt aangeduid als het Big Data-proces. Kunstmatige Intelligentie (KI) richt zich op computers die intelligentie kunnen nabootsen. KI kan voorzien in de technologische handvatten waarmee complexe data-analyses kunnen worden uitgevoerd. Daarmee kan KI van belang zijn voor Big Data-processen en bij het verwerken van data die door met het Internet verbonden apparaten zijn verzameld. De drie technologieën hebben daarnaast gemeenschappelijk dat algoritmes een cruciale technologische bouwsteen vormen in hun functioneren.

De samenkomst van de drie algoritme-gedreven technologische ontwikkelingen kan een grote invloed hebben op het leven van mensen en daarmee op de uitoefening van fundamentele rechten. Dit is vooral zo door de enorme hoeveelheid aan concrete toepassingen. Van de gezondheidszorg en de opsporing van strafbare feiten tot de financiële sector en de ruimtelijke leefomgeving; er is geen domein immuun voor de veranderingen die plaatsvinden onder invloed van Big Data, het IoT en KI, en vooral ook door de invloed van de algoritmes die deze technologieën samenbrengen.

2 Kool e.a. 2017.

Dit onderzoek beoogt primair de effecten van de drie genoemde technologieën voor de grondrechten in beeld te brengen. Alvorens dat te kunnen doen, is het echter nuttig om nadere aandacht te besteden aan de betekenis van respectievelijk Big Data, IoT, KI en de onderliggende algoritmes die het functioneren van deze technologieën bepalen. Deze onderwerpen staan in dit hoofdstuk dan ook centraal. Hierbij wordt de volgende indeling gekozen:

- Paragraaf I.2 richt zich op Big Data. Daarbij wordt ingegaan op de definitie en kenmerken van Big Data, de werking van het Big Data-proces en specifieke toepassingen die aan Big Data gegeven worden.
- Paragraaf I.3 gaat over het IoT. De definitie en kenmerken van het IoT worden besproken. Vervolgens wordt aandacht besteed aan de architectuur van het IoT en ingegaan op concrete toepassingen van deze technologie.
- Paragraaf I.4 ziet op KI. In deze paragraaf worden de definitie en kenmerken van KI uiteengezet. Vervolgens wordt een korte introductie geboden in de deelgebieden van KI, waarbij met name aandacht wordt besteed aan Machine Learning. Ook deze paragraaf sluit af met een illustratie van concrete toepassingen van deze technologie.
- Paragraaf I.5 gaat in op de gemeenschappelijke deler van de drie technologieën: het gebruik van slimme algoritmes.

I.2 Big Data

Data vormen onmisbare bouwstenen voor het vergaren van kennis.[3] Het verzamelen en verwerken van gegevens gebeurt dan ook al sinds jaar en dag. Handmatige volkstellingen en bevolkingsregisters vormen vroege illustraties van het vergaren van kennis door het verzamelen van data op een grote schaal.[4] Het verzamelen en verwerken van data was oorspronkelijk een kostbare en tijdrovende aangelegenheid. Een golf van ontwikkelingen op het terrein van informatie- en communicatietechnologie heeft ertoe geleid dat de mogelijkheden voor het verzamelen en verwerken van gegevens aanzienlijk zijn toegenomen. We leven inmiddels in een 'Data Age'.[5] In 2016 werden evenveel data gegenereerd als in de gehele geschiedenis van de mensheid tot 2015 en de hoeveelheid opgeslagen data zal in 2025 gegroeid zijn tot 163 zettabytes.[6] Bovendien zijn overheden en bedrijven steeds beter in staat om voor besluitvorming relevante informatie uit deze grote hoeveelheid aan data

3 Kitchin 2014, p. 1.
4 Zie hierover Blok 2017, p. 11, WRR 2016, p. 36-37 en White House 2014a, p. 1.
5 White 2015, p. 1.
6 Helbing e.a. 2017 en International Data Corporation 2017, p. 3. Een zettabyte bestaat uit 1.000.000.000.000.000.000.000 bytes (informatie-eenheden). In een poging dit enigszins inzichtelijk te maken, is berekend dat het 1.250 pagina's tellende *Oorlog en Vrede* van Tolstoj 323 biljoen keer in één zettabyte past. Zie White House 2014a, p. 2.

te destilleren. In de hoofdzaak zijn er drie technologische ontwikkelingen die dit mogelijk maken.[7] Ten eerste is de mogelijkheid om gegevens te verzamelen significant gegroeid door de opkomst van de computer in de jaren '50 en '60, het ontstaan van het Internet vanaf 1970 en – vanaf circa 2010 – de opkomst van met het Internet verbonden apparaten. Deze ontwikkeling heeft ertoe geleid dat ons leven zich in toenemende mate online afspeelt.[8] In deze online-wereld kunnen data bovendien eenvoudig worden verzameld en opgeslagen. Ten tweede verdubbelt de capaciteit voor gegevensopslag iedere twee tot drie jaar.[9] Dit maakt dat het technologisch mogelijk is om de verzamelde gegevens op te slaan. Dataopslag is bovendien goedkoper geworden.[10] Ten derde zijn de technologieën om data met elkaar te verbinden en om te zetten naar relevante informatie sterk verbeterd. Zo leidt de toename van data ook daadwerkelijk tot toegenomen kennis. Onder invloed van voorgaande ontwikkelingen is data 'Big' geworden en is 'Big Data' verworden tot een veelgebruikt begrip.

I.2.1 Definitie en kenmerken

Er bestaat geen consensus over de definitie van Big Data. De term wordt door verschillende auteurs en binnen verschillende (wetenschappelijke) disciplines verschillend gedefinieerd.[11] Een vergelijking van deze definities leert dat Big Data veelal wordt omschreven aan de hand van de kenmerken van de gebruikte data en de op deze data toegepaste analysemethodes. Deze kenmerken zijn de hoeveelheid data, de verscheidenheid aan data en de snelheid van dataverzameling en -analyse. Deze elementen vormen de zogeheten '3 V's': *Volume*, *Variety* en *Velocity*.[12]

I.2.1.1 De 3 V's: Volume, Variety en Velocity

Volume (hoeveelheid)

Bij Big Data gaat het om grote hoeveelheden gegevens. Verscheidene definities nemen daarom de hoeveelheid data als uitgangspunt bij het bepalen van wat geldt als Big Data.[13] Tegelijkertijd bestaat er niet iets als een 'minimale' hoeveelheid data, die maakt dat gesproken kan worden van Big Data. Kenmerkend voor Big Data is dat er gestreefd wordt naar verzameling en analyse van een volledige, uitputtende hoeveelheid data (*n=all*).[14] Dit

7 Blok 2017, p. 11-13.
8 Kitchin 2014, p. 80-81.
9 Kool e.a. 2017, p. 41.
10 Kitchin 2014, p. 85.
11 Zie o.a. White House 2014a, p. 2, Lafarre 2016, p. 147 en Wagner 2017, p. 2.
12 Zie o.a. WRR 2016, p. 33, Kitchin & McArdle 2016, p.2 en UK Information Commissioner 2016, p. 2. Laney 2001 is de eerste auteur die Big Data omschreef aan de hand van deze drie kenmerken.
13 Zie bijvoorbeeld McKinsey 2011, p. 1.
14 Kitchin 2014, p. 72.

staat in contrast met traditionele data-analyses, waarbij een beperkte hoeveelheid data wordt verzameld en geanalyseerd. Het verzamelen en analyseren van een volledige populatie is ondoenlijk, dus wordt er een representatieve steekproef genomen. Deze beperking geldt niet bij Big Data, omdat het verzamelen, opslaan en analyseren van grote hoeveelheden gegevens vele malen eenvoudiger is geworden.

Variety (verscheidenheid)

Niet alleen het volume van data is van belang voor de mogelijkheden van (analyse van) Big Data, maar ook de variëteit van de bronnen ervan. Een niet uitputtende lijst van bronnen van data omvat het Internet, sociale media, smartphoneapplicaties, door de overheid beheerde databases, door commerciële bedrijven gegenereerde gegevensbestanden en data verzameld door met het Internet verbonden apparaten.[15] Deze bronnen opereren binnen verschillende domeinen die in toenemende mate onderling verbonden zijn. Die verbondenheid of 'ontschotting' wordt mede veroorzaakt doordat databanken die oorspronkelijk beheerd werden door de overheid of andere grote organisaties in toenemende mate toegankelijk worden gemaakt voor het publiek.[16] Zo kunnen data over het koopgedrag van mensen gebruikt worden om te bepalen of iemand een lening krijgt en kunnen gegevens over iemands fysieke gezondheid worden meegenomen in sollicitatieprocedures.[17] De verscheidene bronnen bevatten daarnaast verschillende 'soorten' data. Zo bestaat er een onderscheid tussen oorspronkelijk analoge en oorspronkelijk digitale data.[18] Oorspronkelijk analoge data komen voort uit de fysieke, offlinewereld en worden vervolgens omgezet naar een digitale vorm. Voorbeelden hiervan zijn stemopnames, met een camera vastgelegde visuele informatie en fysieke activiteit die wordt geregistreerd door een smartwatch. Oorspronkelijk digitale informatie daarentegen is specifiek gecreëerd voor de digitale wereld, zoals het geval is bij e-mail- en Internetverkeer. Een ander relevant onderscheid is dat tussen gestructureerde en ongestructureerde data. 'Gestructureerde data' refereert aan vormen van sterk georganiseerde data, bijvoorbeeld data in een 'relationele database' die is geordend in kolommen en rijen. De 'data-explosie' is echter vooral het gevolg van een toename van zogeheten ongestructureerde data. Dit betreft data die niet zijn weergegeven in strak georganiseerde databases, maar waarbij het bijvoorbeeld gaat om tekst in facebookposts, foto's en video's. Circa 95% van alle data is ongestructureerd.[19]

15 White House 2014a, p. 5.
16 WRR 2016, p. 35 over ontschotting. Over 'open access' data van overheden zie Hardy & Maurushat 2017, p. 30-37.
17 WRR 2016, p. 38-39.
18 In het Engels 'data born analog' en 'data born digital'. Zie White House 2014b, p. 19-23.
19 Gandomi & Haider 2015, p. 138.

Velocity (snelheid)

Big Data wordt ten slotte gekenmerkt door de dynamische aard van het proces waarmee de data worden gegenereerd en geanalyseerd. Waar traditionele data-analyse gebruik moest maken van op een specifiek tijdstip verzamelde data (bijvoorbeeld een periodiek uitgevoerde volkstelling), worden data bij Big Data-analyses constant, veelal *real-time* verzameld en geanalyseerd.[20] Dit betekent dat er direct actie kan worden ondernomen naar aanleiding van de *real-time* data-analyse. Zo houden websites continu bij wie een bezoek brengt aan de website en welke activiteiten door deze persoon op de website worden verricht. De inhoud van de website, bijvoorbeeld de door een webwinkel getoonde aanbiedingen, kan vervolgens direct worden afgestemd op de bezoekersactiviteit. Een dergelijk *real-time*-effect is vaak ook noodzakelijk voor het goed functioneren van websites, applicaties en (andere) informatiesystemen. Zo kan een navigatiesysteem slechts adequaat functioneren als het de gebruiker kan lokaliseren en direct rekening kan houden met actuele verkeersomstandigheden.[21]

Samenspel tussen de 3V's

Er bestaat geen universele 3V-grenslijn, die de overgang van 'Small' naar 'Big' Data markeert. Wat geldt als Big Data kan, in het licht van de snelle technologische vooruitgang, van vandaag op morgen veranderen en verschilt bovendien per sector. Waar de analyse van grote hoeveelheden data in de financiële sector al langer gangbaar is, kan dit in andere sectoren anders liggen.[22] Wel wordt aangenomen dat er een '3V-kantelpunt' bestaat, waarna traditionele methoden van databeheer en -analyse niet langer adequaat kunnen worden toegepast. Waar dit kantelpunt zich bevindt hangt af van de organisatie die Big Data gebruikt en het specifieke toepassingsgebied van de Big Data-analyse.[23] Bovendien bezitten veel datasets die worden geclassificeerd als Big Data niet alle 3 V's of eventuele andere kenmerken. Kitchin en McArdle spreken daarom van het bestaan van 'multiple forms of Big Data'.[24] Big Data wordt aldus eerder beschouwd als een samenspel van kenmerken en ontwikkelingen die bij verschillende datasets in verschillende mate aanwezig zijn, dan als een vastomlijnde technologie.[25]

20 Kitchin 2014, p. 5.
21 White House 2014a, p. 5.
22 WRR 2016, p. 34.
23 Gandomi & Haider 2015, p. 39. Zie in deze trant eveneens UK Information Commissioner 2017, p. 6.
24 Kitchin & McArdle 2016 p. 9, onderzochten dit met betrekking tot zeven karakteristieken van Big Data en kwamen tot de conclusie dat: 'only a handful of datasets possess all seven traits, and some do not possess either volume and/or variety.'
25 Conform de analyse van de WRR 2016, p. 35.

I.2.1.2 Data-gedreven analyse en correlaties

Naast de 3 V's wordt een veelvoud aan andere kenmerken aan Big Data verbonden.[26] Veelgenoemde kenmerken zijn onder meer data-gedreven analyse en de op correlaties georiënteerde aard van Big Data.

Data-gedreven analyse

Oorspronkelijk werden datasets geanalyseerd met als doel het verifiëren van specifieke, vooraf opgestelde hypotheses. De data werden gezien als een middel om antwoord te krijgen op specifieke vraagstellingen, zogeheten *queries*. Zo kan bij het management van een supermarkt de aanname bestaan dat meer mannen dan vrouwen bier aanschaffen. Deze hypothese kan vervolgens worden getest door een *query* te formuleren die de database de opdracht geeft om een lijst te maken met het geslacht van klanten die bier kopen. Uit het resultaat van deze vraagstelling blijkt of de hypothese correct was. Dit voorbeeld geeft aan dat traditionele data-analyse primair hypothese-gedreven is; door mensen vooraf opgestelde, specifieke hypotheses bepalen de bandbreedte van de uit analyse verkregen kennis. Big Data-analyse daarentegen is data-gedreven. Het doel van de data-gedreven analyse is het vinden van relevante patronen en verbanden in datasets. Hiertoe worden algoritmes gebruikt die niet beperkt worden door specifieke hypotheses. Deze algoritmes testen grote hoeveelheden verbanden en proberen op deze wijze relevante informatie uit de data te destilleren. De kennis die vergaard wordt uit data-analyse bevindt zich niet langer uitsluitend binnen de bandbreedte van door mensen opgestelde hypotheses, maar baseert zich primair op wat de data zelf 'zeggen'. Daardoor kunnen waardevolle en onverwachte verbanden ontdekt worden.[27] Een bekend voorbeeld is de data-gedreven analyse van de database van een supermarkt die aantoonde dat klanten die bier kopen vaak eveneens luiers aanschaffen. Toen het management van de supermarkt dit verband ontdekte, werden de schappen met bier dichter bij de luiers gezet, met als gevolg dat de verkoop van bier steeg.[28]

Oriëntatie op correlatie

Het hiervoor gegeven voorbeeld laat al zien dat data-gedreven analyses zich richten op het vinden van statistische verbanden (correlaties), die niet per definitie causaal van aard zijn. Causaliteit betekent dat A de oorzaak is van B, terwijl een correlatie slechts indiceert dat A en B in samenhang voorkomen. In veel situaties zal een statistisch verband een voldoende

26 Kitchin & McArdle 2016, p. 2 verwijzen naar andere 'v-kenmerken' als 'versatility, volatility, virtuosity, vitality, visionary, vigour, viability, vibrancy...virility...valueless, venomous, violating' en een nieuwe categorie aan 'P-woorden': 'portentous, personal, productive, partial, practices, predictive, political, provocative, privacy, polyvalent, polymorphous en playful.'

27 WRR 2016, p. 38; Custers 2017, p. 23; UK Information Commissioner 2017, p. 10.

28 Dit is een befaamde anekdote, die sommigen afdoen als een fabel. Zie Colonna 2013, p. 313.

basis bieden voor het nemen van besluiten. Zo is het vanuit het oogpunt van marketing toereikend om te weten welke personen interesse hebben in bepaalde producten, zonder dat de oorzaak van deze interesse bekend is.[29] Of een correlatie daadwerkelijk toereikend is om daarop besluiten te kunnen baseren, hangt veelal af van het te nemen besluit. Zo ontdekte het bestuur van de Amerikaanse staat Illinois een correlatie tussen de aanwezigheid van boeken bij kinderen thuis en behaalde examenresultaten. Hierop overwoog de gouverneur om ieder kind eens per maand een boek op te sturen. Later bleek echter dat de schoolprestaties van kinderen die boeken tot hun beschikking hadden ook hoger waren als de kinderen de boeken niet lazen. De aanwezigheid van boeken bleek slechts een indicatie voor de prettige studieomgeving die ouders voor hun kinderen wisten te creëren. Er bestond geen causaal verband tussen de aanwezigheid van boeken en studieresultaten.[30] Dit laat zien dat voorzichtigheid betracht moet worden bij het baseren van beslissingen op geconstateerde correlaties.

I.2.2 De werking van het Big Data-proces

Het enkel verzamelen van grote hoeveelheden data is van weinig waarde. Big Data wordt in de praktijk pas nuttig wanneer relevante informatie uit de gegenereerde data kan worden gedestilleerd. Deze informatie kan vervolgens worden gebruikt als basis voor beleids- of besluitvorming.[31] Het gehele proces van kennisvergaring en -benutting wordt aangeduid als het Big Data-proces.[32] De WRR heeft dit proces onderverdeeld in verschillende stappen: verzameling en voorbereiding, analyse en gebruik.[33] Hierna wordt nader ingegaan op de drie te onderscheiden fasen van het Big Data-proces. Hierbij moet in acht worden genomen dat het door de WRR gemaakte onderscheid analytisch van aard is. Door de snelheid waarmee algoritmes werken en het bestaan van constante *feedback loops* zullen de fasen in tijd overlappen en niet altijd logisch opeenvolgend voorkomen.

I.2.2.1 Verzameling en voorbereiding

Wil Big Data-analyse toegevoegde waarde hebben, dan is het van belang data gereed te maken voor analyse. Big Data-analyse is mede mogelijk doordat in de fase van datavoorbereiding een grote verscheidenheid aan data, afkomstig uit verschillende bronnen met

29 Custers 2017, p. 23.

30 Taylor 2013.

31 Zie in deze zin Gandomi & Haider 2015, p. 140.

32 Het proces van kennisvergaring uit databases wordt ook wel aangeduid met de term 'knowledge discovery in databases' ('KDD'). Zie Fayyad, Piatetsky-Shapiro & Smyth 1996. Het hierna beschreven 'Big Data-proces' is gericht op *knowledge discovery* in Big Data.

33 WRR 2016, p. 39 e.v. Het door de WRR omschreven Big Data-proces komt, in verschillende varianten en soms met enkele extra tussenstappen, terug in andere literatuur. Zie bijvoorbeeld Labrinidis & Jagadish 2012.

een verschillende afkomst en structuur samen wordt gebracht. In paragraaf I.2.1.1 is al gerefereerd aan de heterogeniteit van de beschikbare soorten data (oorspronkelijk analoge, oorspronkelijk digitale, gestructureerde en ongestructureerde data). Door middel van *data fusion* kunnen al deze data worden omgezet naar een gestructureerde, homogene dataverzameling.[34] Er bestaat een grote verscheidenheid aan *data fusion*-technieken die het koppelen van verschillende soorten data bewerkstelligen.[35] Door het koppelen van verschillende soorten data worden grote, veelomvattende datasets gecreëerd. Zo was het campagneteam van President Obama in staat om gedetailleerde informatie over campagne-activiteiten te koppelen aan grote hoeveelheden data over de politieke voorkeuren van kiesgerechtigde Amerikanen, hetgeen resulteerde in veelomvattende databases die de gehele kiesgerechtigde populatie van de VS bestreken.[36]

I.2.2.2 Analyse

De analysefase is cruciaal in het Big Data-proces. Zonder analyse zouden grote datasets weliswaar kunnen worden opgeslagen en geraadpleegd, maar zou er geen verschil bestaan tussen input en output.[37] Om de waarde van grote hoeveelheden data te benutten, is het noodzakelijk hieruit relevante informatie te vergaren. Het geheel van technologieën waarmee kennis kan worden vergaard uit grote datasets valt onder de noemer *Big Data analytics*. Hieronder worden enkele van deze technieken uiteengezet. Veel van de beschreven technieken vinden hun grondslag in een deelgebied van Kunstmatige Intelligentie (Machine Learning), dat hierna in paragraaf I.4.1.3 nog aan bod zal komen.

Datamining en profileren

Datamining is een van de voornaamste technologieën die wordt ingezet ten behoeve van Big Data-analyse. Bij datamining worden op geautomatiseerde wijze, door middel van algoritmes, patronen ontdekt in grote datasets.[38] Datamining stelt de gebruiker spreekwoordelijk in staat om door de bomen van data het bos weer te zien.[39] Er bestaan verschillende datamining-algoritmes, die ieder andere correlaties opsporen.[40] Er kan een onderscheid worden gemaakt tussen classificatie-, cluster-, regressie- en associatietechnieken:

– Classificatietechnieken zijn erop gericht om gegevens in verschillende, reeds door programmeurs gecreëerde categorieën onder te brengen. De algoritmes die aan deze techniek ten grondslag liggen 'leren' van een set aan reeds geclassificeerde voorbeelden

34 Boström e.a. 2007 en Custers 2017, p. 26-28.
35 Castanedo 2013.
36 Issenberg 2012 en Crovitz 2012.
37 White House 2014b, p. 24.
38 Custers 2017, p. 28.
39 Colonna 2013, p. 330.
40 Zie over de technieken die worden besproken uitgebreid Calders & Custers 2013 en Hand, Mannila & Smyth 2001 en eveneens Custers 2017, p. 29-30, House 2014b, p. 24-25.

door systematisch verschillen en overeenkomsten tussen de verschillende categorieën te vergelijken. Vervolgens zijn de algoritmes in staat om hieruit regels te destilleren en deze toe te passen op nieuwe gevallen. Zo kunnen uit het ziekenhuis ontslagen patiënten ondergebracht worden in verschillende, vooraf gedefinieerde klassen die indiceren in hoeverre het risico op heropname aanwezig is. Ook spam-filters zijn een goed voorbeeld van dit type algoritmes. Op basis van een analyse van een grote set van als spam gekwalificeerde mails, kan nieuw inkomende spam met een hoge mate van zekerheid worden geïdentificeerd. Vervolgens worden mails die zijn geclassificeerd als spam, automatisch in de spam-box geplaatst; de mails die niet als spam zijn geclassificeerd, verschijnen in de inbox.

- Bij clustertechnieken richten algoritmes zich op het groeperen van gegevens die sterk overeenkomen. Zo kan het klantenbestand van een winkel aan de hand van hun aankoopgedrag worden onderverdeeld in subgroepen met 'typen' klanten. Het verschil tussen classificatie- en clustertechnieken is dat classificatie gebaseerd is op reeds bestaande, van te voren gedefinieerde klassen, terwijl clustering erop is gericht dergelijke klassen te creëren op basis van de data-analyse. Sterk verwant aan clusteren is het opsporen van zogenaamde 'uitbijters' (*outlier detection*). Dit betekent dat een algoritme onregelmatigheden in data ontdekt. Zo kan de belastingdienst atypische (mogelijk frauduleuze) aangiften herkennen en deze aan nader onderzoek onderwerpen.
- Regressietechnieken formuleren numerieke voorspellingen op basis van in datasets geïdentificeerde verbanden. Zo kan Facebook voorspellen hoe groot de kans is dat een gebruiker in de toekomst actief zal zijn, door het analyseren van reeds beschikbare gegevens als de hoeveelheid gedeelde persoonlijke informatie en het aantal berichten dat deze persoon *liket*. Een ander voorbeeld is een bank die kan voorspellen hoe groot de kans is dat een lening niet wordt terugbetaald met behulp van een algoritme en op basis van gegevens bij het aanvragen van een lening.
- Bij associatietechnieken zoeken algoritmes naar correlaties tussen gegevens en worden op basis van deze correlaties associatieregels geformuleerd, die bijvoorbeeld als aanbevelingen aan klanten kunnen worden gepresenteerd. De aanbevelingstechnieken van Amazon en Netflix (als u dit interessant vindt, bent u mogelijk ook geïnteresseerd in …) werken op basis van associatie-algoritmes.

Een andere relevante en sterk aan datamining verwante techniek is profileren (*profiling* of profilering). Algoritmes worden daarbij ingezet om profielen op te stellen, waaronder van personen of groepen van personen.[41] Aan profilering liggen veelal dataminingtechnieken ten grondslag. Om die reden wordt profileren ook wel gezien als op personen toegepaste

41 Custers 2013, p. 7-15.

datamining.[42] Binnen profilering kan globaal onderscheid worden gemaakt tussen groepsprofielen en persoonsprofielen:[43]

- Een persoonsprofiel bestaat uit een verzameling van eigenschappen (ook wel 'attributen') van een persoon. Een voorbeeld is het profiel van mevrouw Jansen, die 46 jaar oud is, vier kinderen heeft en €45.000 per jaar verdient. Bij het verder verfijnen van een persoonsprofiel kan datamining worden ingezet om attributen te voorspellen. Zo kunnen op basis van de berichten die mevrouw Jansen *liket* op Facebook haar seksuele voorkeur, etniciteit, politieke voorkeur, intelligentie, geluk en mogelijke drugsproblematiek worden voorspeld.[44] Voor het opstellen van een individueel profiel is de hiervoor beschreven regressietechniek geschikt.
- Een groepsprofiel bestaat uit een verzameling attributen van een groep personen. Bij een zogeheten distributieve groep zijn de attributen van de groep aanwezig bij alle personen die zich in de groep bevinden. Zo is 'niet getrouwd zijn' een attribuut van alle personen in de groep vrijgezelle Nederlanders. De meeste groepsprofielen kennen een niet-distributief karakter. Dit betekent dat de voor de groep geldende attributen niet noodzakelijkerwijs voor alle individuen in de groep gelden. Dergelijke attributen worden vaak uitgedrukt in gemiddelden en percentages. Zo kan een groep personen met een bepaalde postcode gemiddeld €60.000 verdienen. Dit betekent echter niet dat alle personen in deze groep dit inkomen hebben. Een ander voorbeeld betreft een groepsprofiel van personen met blauwe ogen en rood haar, waarvan berekend is dat de kans op het krijgen van een specifieke huidziekte 88% bedraagt. Dit betekent echter niet dat iedere persoon in deze groep deze kans op de huidziekte heeft en al helemaal niet dat deze kans ook wordt verwezenlijkt, omdat dit af kan hangen van individuele factoren als leeftijd, eetgewoonten en het aantal uren dat een persoon doorbrengt in de zon.[45] *Profiling* kan door het maken van groepsprofielen ook worden gebruikt voor het opstellen van risicoprofielen, bijvoorbeeld ten aanzien van de kans dat iemand zijn lening niet terugbetaald of een terrorist is. Voor het opstellen van deze profielen wordt veelal gebruikgemaakt van classificatie- en clusteralgoritmes.

Uit het voorgaande blijkt dat datamining en profileren op verscheidene manieren ingezet worden ten behoeve van data-analyse. Op hoofdlijnen kan een onderscheid worden gemaakt tussen voorspellende en beschrijvende analyses:

- Technieken gericht op voorspellende analyse worden ook wel begeleide of gestuurde analyses genoemd.[46] Deze analyses vinden plaats in twee stappen. Eerst wordt een

42 WRR 2016, p. 44.
43 Hildebrandt 2006, p. 549; Hildebrandt 2008, p. 20-23.
44 Kosinskia, Stillwella & Graepel 2012.
45 Hildebrandt 2006, p. 549.
46 Schermer 2011, p. 46.

algoritme 'getraind' door het bloot te stellen aan een reeks geclassificeerde voorbeelden. Deze 'oefendata' kunnen bijvoorbeeld bestaan uit gegevens over personen, waarvan enkele geclassificeerd zijn als terrorist. Vervolgens wordt het algoritme losgelaten op een nieuwe set aan data en is het in staat om op basis van correlaties en vergelijkbaarheid met de voorbeelden, nieuwe gevallen te classificeren. Het algoritme kan op deze wijze een voorspelling doen over kenmerken van een specifiek object in de data. Zo kan een algoritme in het gegeven voorbeeld op basis van een nieuwe set aan gegevens voorspellen welke personen als terrorist aangemerkt kunnen worden. Voor voorspellende analyses worden meestal classificatie- en regressietechnieken ingezet.

– Beschrijvende datamining en profilering richten zich op het verschaffen van een beter begrip van de data en het ontdekken van verbanden binnen een dataset. Hiervoor worden vooral cluster- en associatietechnieken ingezet. Beschrijvende analyses worden ook wel onbegeleide of ongerichte analyses genoemd.[47] Dat wil zeggen dat een algoritme niet vooraf getraind wordt en het niet tot doel heeft om een bepaald object te kwalificeren. Wel kan een descriptieve analyse worden verbonden met een zogeheten prescriptieve analyse. Op basis van de uitkomst van een voorspellende analyse kan dan een bepaalde handelswijze worden voorgeschreven.[48]

Andere technieken

Naast datamining en profileren bestaat een reeks andere technieken die worden ingezet voor Big Data-analyse.[49] Deze technieken zijn sterk gelieerd aan en veelal gebaseerd op de hiervoor omschreven technieken en het gebruik van algoritmes daarbij. Hieronder worden enkele van deze technieken kort toegelicht.

– Tekstanalyse stelt de gebruiker in staat om relevante informatie te vergaren uit grote hoeveelheden ongestructureerde tekst, zoals berichten op sociale media en online fora of grootschalige enquêtes. Twee voorbeelden hiervan zijn *text summarisation* en *sentiment analysis.* De eerste techniek gebruikt algoritmes die in staat zijn om samenvattingen te produceren van (meerdere) grote stukken tekst. De tweede techniek wordt ook wel *opinion mining* genoemd en richt zich op het analyseren van opiniërende teksten over producten, bedrijven, personen en evenementen. Zo kan het voor politieke partijen van belang zijn om informatie te krijgen over op sociale media geuite commentaren tijdens een verkiezingsdebat en streven bedrijven naar een effectieve analyse van productbeoordelingen.[50]
– Door middel van spraak- en afbeeldingsherkenning kan informatie worden verkregen uit een veelheid aan (audio)visueel materiaal. Zo gebruiken callcenters algoritmes om

47 Idem, p. 46.
48 WRR 2016, p. 44.
49 Zie over deze technieken White House 2014b, p. 24-30 en Gandomi & Haider 2015, p. 140-144.
50 Zie ter illustratie respectievelijk Sharma, Mittal & Garg 2016 en Fan & Wu 2011.

duizenden uren aan opgenomen telefoongesprekken te analyseren. Deze analyses kunnen vervolgens worden ingezet om de klanttevredenheid te verhogen of om te monitoren of verkopers zich houden aan het geldende privacybeleid. Andere technieken richten zich op het doorzoeken van duizenden uren aan videomateriaal, bijvoorbeeld ten behoeve van de opsporing van strafbare feiten.

– Sociale media-analyses richten zich op de gestructureerde en ongestructureerde data die worden gegenereerd op sociale media als Facebook, LinkedIn, Twitter, Instagram en YouTube. Dit type analyse kan worden onderverdeeld in een tweetal categorieën: inhoudgebaseerde en structuurgebaseerde analyses. Waar inhoudgebaseerde analyses zich richten op de door gebruikers geplaatste 'content', kunnen structuurgebaseerde analyses de relaties tussen de verschillende gebruikers onderzoeken. Door middel van deze technieken kunnen bijvoorbeeld sub-netwerken worden geïdentificeerd van gebruikers die veel contact met elkaar hebben en kan de invloed van specifieke actoren op sociale media worden bijgehouden.

Menselijke betrokkenheid

Big Data-analyse vindt plaats met behulp van algoritmes, die 'zelflerend' kunnen zijn en zichzelf verder kunnen ontwikkelen op basis van de uitkomsten van de uitgevoerde analyses.[51] Betrokkenheid van menselijke actoren is echter onmisbaar voor het goed functioneren van data-analyses. Algoritmes worden bedacht, geprogrammeerd en – waar nodig – getraind door mensen. Daarnaast is menselijke betrokkenheid nodig om de verkregen resultaten te interpreteren en te beoordelen op relevantie en geldigheid.[52] Zoals al is opgemerkt is niet ieder gevonden verband immers causaal van aard; veel correlaties zijn voor het nemen van besluiten helemaal niet relevant. Mensen zullen ook moeten helpen om een balans te vinden tussen te smalle of te brede analyses. Waar bij te smalle analyses weinig nieuwe kennis uit data zal worden verkregen, leiden te brede analyses sneller tot irrelevante of reeds bekende verbanden. Menselijke intuïtie is nodig om het beste evenwicht hiertussen te bepalen.[53]

I.2.2.3 Gebruik

Het uiteindelijke doel van Big Data-analyse is het faciliteren van *evidence-based decison-making*. Een analyse leidt tot *actionable knowledge*, waarbij op basis van uit de analyse verkregen inzichten besluiten kunnen worden genomen of beleid kan worden gemaakt. Deze fase van het gebruik van de uitkomsten van de data-analyses is getypeerd als de minst

51 Op zelflerende algoritmes wordt in paragraaf 5 nader ingegaan.
52 Colonna 2013, p. 335-336.
53 Custers 2017, p. 22-23.

technische, maar wel als de belangrijkste fase vanuit een maatschappelijk perspectief.[54] Er kan daarbij onderscheid worden gemaakt tussen de fase voorafgaand aan de besluitvorming en de fase van eigenlijke besluitvorming.[55]

De fase voorafgaand aan de besluitvorming
De inzichten die uit een data-analyse worden verkregen kunnen worden meegenomen bij het ontwikkelen van besluitvormingsmodellen of algoritmes. De uit analyse verkregen resultaten worden dan gebruikt voor de optimalisering van nieuwe analyses. De Hert, Lammerant en Blok illustreren dit met het volgende voorbeeld: de analyse van een dataset van een elektronicawinkel toont aan dat er een statistisch verband bestaat tussen de grootte van het televisiescherm dat iemand koopt en de tijd die het duurt om de lening terug te betalen die is afgesloten voor de televisie. Naar aanleiding van deze bevinding kan schermgrootte worden toegevoegd aan het algoritme dat bepaalt of en onder welke voorwaarden iemand een televisie op krediet kan kopen.[56] Bij slimme algoritmes vindt dit proces automatisch plaats.[57] Via zogenaamde *feedback loops* kunnen deze algoritmes zichzelf aanpassen aan de resultaten van eerder uitgevoerde analyses.

De besluitvorming
Sommige besluiten volgen automatisch uit Big Data-analyse. Zo raadt Netflix zonder menselijke tussenkomst bepaalde films aan op basis van een associatie-analyse van eerder bekeken series of films. Ook een real-time verkeersanalyse in een navigatiesysteem leidt tot directe adviezen aan de bestuurder. Kenmerkend voor deze twee voorbeelden van Big Data-analyse is dat het weinig ingrijpende adviezen betreft. In de loop van deze paragraaf zijn echter ook voorbeelden de revue gepasseerd die meer dwingend van aard zijn en potentieel een grote invloed op de levens van mensen kunnen hebben. Zo kan de op een algoritme gebaseerde beslissing om iemand geen lening of hypotheek toe te kennen, drastische gevolgen hebben voor iemands financiële situatie. De beslissing om strafvorderlijke maatregelen te treffen tegen een persoon op basis van de door een algoritme bepaalde kwalificatie van deze persoon als terrorist, is van een nog ingrijpender aard. Dit toont aan dat beslissingen die (al dan niet (semi-)automatisch) gebaseerd kunnen worden op Big Data-analyse, potentieel grote consequenties kunnen hebben. In hoofdstuk III wordt daarop verder ingegaan voor zover het gaat om de potentiële gevolgen voor grondrechten.

54 WRR 2016, p. 45. Daarbij moet worden aagetekend dat ook bij – bijvoorbeeld – het ontwerp van de algoritmes die ten grondslag liggen aan Big Data-analyse, alsmede bij dataverzameling belangrijke keuzes worden gemaakt die uiteindelijk doorwerken in de uitkomst van de analyse en in het gebruik daarvan. De uitspraak van de WRR geeft vooral aan dat de exacte wijze waarop uiteindelijk wordt omgesprongen met de uitkomsten van Big Data-analyses van groot maatschappelijk belang is.
55 De Hert, Lammerant & Blok 2017, p. 124.
56 Idem.
57 Zie over dergelijke algoritmes nader paragraaf I.5.

I.2.3 Toepassingen

Anno 2018 wordt Big Data ingezet op een veelheid aan terreinen. Om inzicht te geven in concrete Big Data-toepassingen worden in deze paragraaf voorbeelden gegeven van de (potentiële) aanwezigheid van Big Data binnen een aantal (overlappende) maatschappelijke en commerciële domeinen. Op hoofdlijnen wordt een onderscheid gemaakt tussen toepassingen in de publieke en private sector. Hierbij moet worden aangetekend dat het door geheimhouding en het experimentele karakter van sommige toepassingen niet eenvoudig is om een volledig beeld te krijgen van Big Data-toepassingen.[58] Het overzicht dat volgt is geenszins uitputtend, maar dient slechts ter illustratie van de veelomvattende aanwezigheid van Big Data.

I.2.3.1 Publieke sector

Veiligheidsdomein

In Nederland zijn enkele treffende voorbeelden te vinden van de inzet van Big Data-toepassingen in het veiligheidsdomein.

– *Predictive policing* is het voorspellen van crimineel en normoverschrijdend gedrag door middel van grootschalige verzameling, verwerking en analyse van data.[59] Voorspellende data-analyse wordt hierbij ingezet ter ondersteuning van de opsporing. *Predictive policing* richt zich op het voorspellen van criminele activiteiten, mogelijke daders en/of mogelijke slachtoffers.[60] Tot op heden wordt *predictive policing* in de opsporingspraktijk met name gebruikt om een effectieve politie-inzet te realiseren. Met behulp van Big Data-analyse kan worden bepaald welke straten, groepen of individuen extra controle behoeven.[61] Op basis van ingevoerde data, zoals datum, tijdstip, type delict en locatie kan met behulp van een algoritme worden berekend waar de kans op het plaatsvinden van het betreffende type delict het grootst is. De nationale politie heeft groot vertrouwen in voorspellende Big Data-analyse. *Predictive policing* kan worden gezien als de toekomstige basis van het nemen van beslissingen over het politiewerk.[62] Het Criminaliteits Anticipatie Systeem (CAS) is de Nederlandse toepassing van *predictive policing*. Het CAS verdeelt Nederland in rastervakjes van 125 bij 125 meter. Van ieder vakje wordt een grote hoeveelheid gegevens verzameld, zoals specifieke locatiegegevens van het raster (de afstand tot de woonplaats van bekende verdachten, de afstand tot de dichtstbijzijnde snelwegoprit, soort en aantal bedrijven, gokhallen en cafés), demogra-

58 WRR 2016, p. 128.
59 Over predictive policing is veel academische literatuur beschikbaar. Zie o.a. Perry 2013, Miller 2014 en Willems 2014.
60 Lodder e.a. 2014, p. 65.
61 Mayer - Schonberger & Cukier 2013, p. 158.
62 Lodder & Schuilenburg 2016, p. 153 onder verwijzing naar Rienks 2015.

fische en sociaaleconomische gegevens (gemiddeld buurtinkomen) en historische data over woninginbraken en andere criminele incidenten.[63] Op basis van deze gegevens worden zogeheten *heat maps* weergegeven, die laten zien waar de kans op bepaalde type delicten het grootst is. Deze informatie wordt vervolgens gebruikt om tot een optimale allocatie van politie-inzet te komen en misdaad te voorkomen. In mei 2017 kondigde de Nationale Politie aan om het CAS verder uit te rollen. Ruim 90 basisteams gaan met het CAS werken.[64]

– *Webcrawling* is een toepassing van datamining waarbij het Internet methodisch en automatisch kan worden doorzocht op verdacht materiaal.[65] De techniek kan bijvoorbeeld worden ingezet voor het analyseren van de achtergrond van een verdachte of het opsporen van beeldmateriaal van vuurwapens of kinderporno.[66] De politie zet het systeem iColumbo in om aan de hand van bepaalde trefwoorden of profielen het Internet te doorzoeken met het oog op de opsporing van strafbare feiten. De dataverzameling wordt door iColumbo geordend en geprioriteerd. Het handmatig doorzoeken van het Internet is met iColumbo niet langer nodig.[67]

Belastingen

De belastingdienst is een koploper in het gebruik van Big Data-technieken binnen de overheid. Aandacht verdient met name de notie van 'informatiegestuurd toezicht', waarbij data-analyses worden ingezet om fraude te bestrijden en gerichte controles uit te voeren.[68] De Belastingdienst zet Big Data-analyse onder meer in om 'risicoscores' bij de aanvraag van toeslagen te formuleren, om verkeerd ingevulde aangiften te traceren en om 'green lanes' te creëren voor (rechts)personen die hun aangiften juist invullen.[69] Door Big Data-analyse is de Belastingdienst in staat om (illegale) onvolkomenheden in belastingaangiftes te voorspellen en hierop preventieve en controlerende maatregelen af te stemmen. Het hiervoor genoemde iColumbo-systeem wordt ook door de Belastingdienst gebruikt bij het onderzoeken van fraude en het uitvoeren van background checks van (rechts)personen bij goederenvervoer.[70]

63 WRR 2016, p. 50.
64 'Criminaliteits Anticipatie Systeem verder uitgerold bij Nationale Politie', via: https://www.politie.nl/nieuws/2017/mei/15/05-cas.html (laatst geraadpleegd 3 januari 2018).
65 Lodder & Schuilenburg 2016, p. 150. Zie uitgebreid over *webcrawlers* Boonk & Lodder 2006.
66 Lodder 2014, p. 71.
67 Brinkhoff 2016. Zie nader over iColumbo Koops e.a. 2012, p. 7.
68 Van Hout 2017, p. 1037.
69 WRR 2016, p. 52.
70 Van Hout 2017, p. 1036-1037.

Onderwijs

Al vroeg werd erkend dat datamining een nuttige functie kan vervullen binnen het (hoger) onderwijs. Het is voor onderwijsinstellingen van groot belang om het leerproces van hun studenten te kunnen volgen en relevante verbanden te kunnen leggen tussen studieresultaten en andere gegevens.[71] Door middel van *learning analytics* kunnen studiedata worden verzameld en geanalyseerd, waarbij de resultaten vervolgens van grote waarde zijn bij het bevorderen van onderwijskwaliteit en bij onderwijsmonitoring. Hildebrandt geeft het voorbeeld van MyStatLab, waarbij 'Big Leerdata' van Blackboard en andere grootschalige e-learning-onderwijsapplicaties worden gebruikt om kennis te vergaren over leerprocessen. Big Data maakt het mogelijk om verbanden te leggen tussen gedrag en onderwijsprestaties, 'bij wijze van spreken tussen het eetpatroon van studenten en hun scores'. [72] Dit leidt ertoe dat mogelijk relevante correlaties worden ontdekt tussen studieprestaties en een veelheid aan (persoonlijke) karakteristieken als sociaaleconomische achtergrond, etniciteit, leeftijd en geslacht. Deze verbanden kunnen in theorie ten grondslag worden gelegd aan beslissingen over studieondersteuning en toelatingsbeleid.

Sociale zekerheid

Binnen het socialezekerheidsdomein is het tegengaan van fraude met publieke gelden van groot belang. Het Systeem Risico Indicatie (SYRI) dient ter voorkoming en bestrijding van misbruik van overheidsgelden binnen de sociale zekerheid. SYRI wordt gebruikt door een samenwerkingsverband van gemeenten, het UWV, de Sociale Verzekeringsbank, de Inspectie SZW en de Belastingdienst. Het SYRI kan een groot aantal gegevensbestanden met elkaar combineren, variërend van arbeidsgegevens tot zorgverzekeringsgegevens en fiscale gegevens, om zo fraude te signaleren. De gegevensanalyse door het SYRI gebeurt in twee fasen: eerst worden relevante datasets door het zogeheten 'Inlichtingenbureau' aan elkaar gekoppeld en 'gematcht' met een onder verantwoordelijkheid van de minister (feitelijk door de Inspectie SZW) ingericht risicomodel. Vervolgens worden potentiële treffers nogmaals geanalyseerd door medewerkers van de Inspectie SZW, die bepalen welke personen of gegevens voor een risicomelding in aanmerking komen en dit doorgeven aan de betrokken instanties. Deze instanties zijn verplicht te onderzoeken of er daadwerkelijk sprake kan zijn van fraude, voordat een sanctie kan worden opgelegd.[73]

De mogelijke inzet van Big Data-analyse in de sociale zekerheid beperkt zich niet tot handhavingsbeleid.[74] Zo kunnen profileertechnieken worden ingezet om werkloosheid tegen te gaan. McKinsey wijst in dat kader op het Duitse *Bundesagentur für Arbeit*, dat

71 Luan 2004. Zie ook White House 2014a, p. 24-27.
72 Hildebrandt 2016a; Hildebrandt 2016b.
73 Evers 2016, p. 168-169 en WRR 2016, p. 56-58.
74 Zie in het algemeen Balasubramanian 2015, p. 15-21.

grote hoeveelheden data analyseerde over werkzoekenden en de ondersteuning die de Duitse overheid aan deze werkzoekenden had geboden. Dit stelde het *Bundesagentur* in staat deze personen ondersteuning op maat aan te bieden.[75] Een soortgelijk voorbeeld is het Poolse systeem, waarin werkzoekenden worden ingedeeld in drie categorieën.[76] De indeling in een categorie is bepalend voor de ondersteuning die een persoon krijgt bij het vinden van werk. De indeling geschiedt op basis van 'persoonlijke kenmerken' die worden bepaald door het invullen van een computergestuurd interview met de werkzoekende. Een algoritme bepaalt, op basis van een veelheid aan beschikbare data en het interview, de categorisering van de betreffende werkzoekende.

Politiek
Het voorbeeld van de verkiezingscampagne van President Obama toont aan dat Big Data-analyse van groot belang kan zijn binnen het politieke domein. In een politieke setting kunnen Big Data-technieken onder meer worden gebruikt bij het uiteenzetten van een campagnestrategie, het analyseren van de invloed van politici en het opstellen van kiezersprofielen.[77]

I.2.3.2 Private sector

Financiële sector en verzekeringsbranche
De toepassing van Big Data-analyse in de financiële wereld is veelomvattend en wijdverspreid. In de bancaire sector behoren het opsporen van kredietfraude en het uitvoeren van risico-inventarisaties van potentiële klanten tot voorname toepassingen van datamining. Citron en Pasquale geven aan dat zogeheten 'credit scores' en de onderliggende algoritmes het economische lot van miljoenen individuen bepalen.[78] Het berekenen van de kredietwaardigheid geschiedt door het loslaten van een algoritme op een bepaalde set aan variabelen, bijvoorbeeld iemands betaalgeschiedenis, uitstaande schulden en de verhouding tussen het vermogen van de kredietaanvrager en de hoogte van de lening. Aan iedere variabele wordt een numerieke waarde verbonden, die in samenhang de kredietscore bepalen. Met het beschikbaar worden van grotere hoeveelheden data, kunnen tegenwoordig ook andere gegevens worden meegenomen. Het kan hierbij bijvoorbeeld gaan om sociale-mediagegevens, algehele uitgavenpatronen, opleiding en telefoonrekening. Big Data-analyse stelt financiële instellingen in staat grote hoeveelheden gevarieerde data te verwerken in

75 McKinsey 2011, p. 59.
76 Niklas, Sztandar-Sztanderska & Szymielewicz 2015.
77 Colonna 2013, p. 358. Zie in dit verband ook Staatscommissie parlementair stelsel 2017, p. 49 e.v.
78 Citron & Pasquale 2016, p. 8.

de kredietbeoordeling.[79] In het verzekeringswezen wordt eenzelfde soort techniek toegepast, op basis waarvan uitgebreide risicotaxaties worden gemaakt bij het berekenen van premies en uitkeringen.[80] Naast voorgaande toepassingen behoort het voorspellen van bijvoorbeeld de waarde van aandelen, opties en derivaten, tot de kern van de toepassing van Big Data in de financiële wereld.[81]

Commerciële sector (retail en marketing)
Big Data-technieken kunnen bijdragen aan de winstgevendheid van commerciële ondernemingen. McKinsey wijst bijvoorbeeld op een zestiental Big Data-technieken die door (online) winkels gebruikt kunnen worden ingezet ten behoeve van omzetmaximalisatie.[82] Zo kan Big Data-analyse worden ingezet om bestaande klanten meerdere producten te laten kopen (*cross-selling*). Het door Amazon gebruikte associatie-algoritme biedt hiervan een treffend voorbeeld. Ook op andere manieren kan marketing worden afgestemd op individuele (potentiële) klanten op basis van hun online gedrag (*behavioural targeting*).[83] Hierbij kan gebruik worden gemaakt van bijvoorbeeld de real-time locatie van de klant (*location-based marketing*) of zijn of haar huidige sentiment blijkend uit berichten die de klant plaatst op sociale media (*sentiment analysis*). De analyse van het 'in-store' gedrag van klanten kan behulpzaam zijn bij het inrichten van een winkel. Ook de prijzen van producten of diensten kunnen worden afgestemd op individuen of groepen van klanten (*price discrimination* of *price optimalisation*).[84] Een overkoepelende techniek die in dit kader van belang is, is de zogeheten *consumer profiling*. Op basis van data-analyse kan een zeer gedetailleerd profiel van een consument worden opgesteld. Dit profiel kan bestaan uit daadwerkelijk bestaande of door middel van analyse voorspelde karakteristieken van de specifieke consument. Marketing- en verkoopstrategieën kunnen vervolgens 'op maat' worden ingezet.[85]

Human Resources
In het personeelsbeleid kan Big Data-analyse een belangrijke rol spelen. Big Data kan onder andere worden ingezet om het toekomstige succes van (potentiële) werknemers te voorspellen.[86] Dit kan met name van nut zijn voor werving en selectie. Big Data stelt ondernemingen (en de overheid als werkgever) bovendien in staat om naar veel meer te kijken dan

79 Hurley & Adebayo 2016, p. 162-166 met een overzicht van door verscheidene kredietbeoordelaars gebruikte criteria.
80 Kemp 2014, p. 484-485.
81 Colonna 2013, p. 353.
82 McKinsey 2011, p. 67-71.
83 Zuiderveen Borgesius 2014, p. 28.
84 Zie Steppe 2017; Zuiderveen Borgesius & Poort 2017.
85 King & Forder 2016.
86 Colonna 2013, p. 357.

slechts cijfers, diploma's en de resultaten van een assessment bij het aannemen van nieuwe werknemers. Ook activiteit op sociale media, of een tekstanalyse van het cv of een sollicitatiebrief kunnen worden meegenomen. De uitkomst van de op een algoritme gebaseerde analyse kan vervolgens (mede) bepalen wie voor een sollicitatiegesprek wordt uitgenodigd of wordt aangenomen. Het werk van recruiters blijkt deels al overgenomen te kunnen worden door algoritmes. Uit een analyse van 440.000 cv's blijkt dat een algoritme met 80% zekerheid kan voorspellen welke kandidaten door recruiters op gesprek zullen worden uitgenodigd. Het algoritme is eveneens in staat te beoordelen welke kandidaten geschikt zijn voor specifieke functies.[87]

Sociale media en zoekmachines

Er zijn reeds veel voorbeelden gegeven van manieren waarop de via sociale media beschikbare data kunnen worden benut voor Big Data-analyses. Big Data-processen worden ook ingezet *door* sociale-mediabedrijven. Facebook, Instagram, Twitter, YouTube, Tumblr, Pinterest, LinkedIn en andere bedrijven streven naar optimaal gebruik van de grote hoeveelheden data die hun gebruikers genereren. Een bekend voorbeeld van de toepassing van een algoritme dat wordt toegepast op grote hoeveelheden door gebruikers gegenereerde data is de gepersonaliseerde tijdlijn van Facebook. Op basis van *likes*, gevolgde pagina's, informatie over facebook-vrienden, interactie met websites en het apparaat dat wordt gebruikt om facebook te bezoeken krijgt iedere Facebookgebruiker een eigen, gepersonaliseerde *newsfeed* te zien. Deze tijdlijn bevat informatie die Facebook relevant acht op basis van het unieke profiel van de gebruiker dat Facebook heeft opgesteld.[88] Het algoritme kan door Facebook worden aangepast om veranderingen in de *newsfeed* van individuele gebruikers te bewerkstelligen. YouTube-aanbevelingen, Instagram-suggesties en vacatures die LinkedIn laat zien zijn eveneens afgestemd op de individuele gebruiker door middel van een algoritme.[89] Zoekmachines als Google maken verder gebruik van complexe algoritmes om zoekresultaten te personaliseren en prioriteren.[90] Google zelf stelt dat het uitgebreid gemaakt maakt van 'new algorithmic ideas to impact millions of users'.[91] De advertenties die op sociale media en via zoekmachines worden getoond zijn vormen van *behavioural targeting*. Advertenties worden daarbij afgestemd op zoekslagen die gebruikers in

87 Lee 2016.

88 Zie over deze vorm van vooraf geselecteerde personalisatie Zuiderveen Borgesius e.a. 2016.

89 Zie, ten aanzien van YouTube, bijv. Covington, Adams & Sargin 2016.

90 Zie 'How Google Finds Your Needle in the Web's Haystack', online via: http://www.ams.org/samplings/feature-column/fcarc-pagerank?_sp=9196e030-64b1-48f4-b4f9-5be2ea3f7a1.1515597204154 (laatst geraadpleegd 22 januari 2018).

91 Respectievelijk Research at Google, 'Algorithms and Theory', via: https://research.google.com/pubs/AlgorithmsandTheory.html en Research at Google, 'Data mining and modelling', via: https://research.google.com/pubs/DataMiningandModeling.html (laatst geraadpleegd 22 februari 2018).

een zoekmachine hebben ingevoerd of op de pagina's die een persoon op sociale media heeft geliket.

I.2.3.3 Proliferatie van Big Data toepassingen

Door voortschrijdende technologische ontwikkelingen zal Big Data-analyse niet langer voorbehouden zijn aan 'grote', invloedrijke en financieel daadkrachtige organisaties. Blok constateert dat 'de infrastructuur om gegevens op te slaan en te verwerken niet alleen ter beschikking [staat] aan grote organisaties en ondernemingen, maar ook aan MKB-bedrijven en particulieren.'[92] In de toekomst valt dan ook een proliferatie van Big Data-toepassingen te verwachten, waarbij Big Data wordt gebruikt door een veelheid aan overheidsinstanties, ondernemingen en particulieren.

I.3 Internet of Things

Het met het Internet verbinden van 'dingen', dateert van voor het gebruik van de term Internet of Things (IoT). In de vroege jaren 80 monteerden studenten in de Verenigde Staten met het Internet verbonden fotosensoren in een frisdrankautomaat.[93] Dit stelde iedereen met toegang tot het Internet in staat om het aantal verkochte (en resterende) blikjes te tellen. Reeds in 1990 werd op een grote technologieconferentie een broodrooster gepresenteerd dat door middel van het Internet aan en uit kon worden gezet.[94] Pas in 1999 introduceerde de Britse technologie-pionier Kevin Ashton de term Internet of Things.[95] Ashton duidde met dit begrip een systeem aan waarbij producten worden voorzien van een Radio-Frequency Identification (RFID)-tag die in verbinding staat met het Internet. Daarmee kunnen bijvoorbeeld producten in een bevoorradingsketen worden geteld en gelokaliseerd, zonder menselijke tussenkomst. De laatste jaren heeft het IoT een enorme vlucht genomen. Er wordt geschat dat in 2020 wereldwijd 20 miljard apparaten met het Internet verbonden zullen zijn.[96] De totale geschatte waarde van de 'IoT-industrie', loopt op tot 11,1 triljoen dollar in 2015.[97]

92 Blok 2017, p. 12.
93 Vetter 1995.
94 Maple 2017, p. 155-156.
95 Ashton 2009.
96 Gartner 2017. Voor eerdere andere schattingen zie Kool e.a. 2017.
97 McKinsey 2015.

I.3.1 Definitie en kenmerken

Verschillende definities benadrukken verschillende aspecten van het IoT.[98] In een zeer brede opvatting wordt het IoT gezien als het geheel van op het Internet aangesloten apparaten.[99] Specifieker zijn definities die zich richten op 'alledaagse' apparaten of, in andere woorden, apparaten die oorspronkelijk niet tot de categorie computers worden gerekend. De gemeenschappelijke deler in de definities wordt door The Internet Society als volgt samengevat:

> 'The terms 'Internet of Things' and 'IoT' refer broadly to the extension of network connectivity and computing capability to objects, devices, sensors and items not ordinarily considered to be computers.'[100]

De Oxford Dictionary biedt een soortgelijke definitie:

> 'Internet of things (noun): The interconnection via the Internet of computing devices embedded in everyday objects, enabling them to send and receive data.'[101]

De ontwikkeling van het IoT is een resultaat van de samenkomst en snelle evolutie van reeds langer bestaande technologieën.[102] Deze technologieën worden hieronder besproken aan de hand van twee definiërende kenmerken van het Internet of Things: de 'everyday objects' die samen het IoT vormen, en het 'Internet' waarmee zij worden verbonden.

I.3.1.1 'Internet'

Het Internet is het wereldwijde netwerk van computers dat door middel van schakelaars, routers, kabels, glasvezel, communicatiesatellieten en andere fysieke apparatuur in staat is tot onderlinge communicatie. De primaire functie van het Internet is het transporteren van informatie van het ene naar het andere punt op een snelle, betrouwbare en veilige manier. Het World Wide Web (www) is een specifieke toepassing van het Internet. Het is een 'grafische interface' die gebruikers in staat stelt op eenvoudige, bruikbare wijze via

98 Weber & Studer 2016, p. 718. Zie in dat kader de gezaghebbende definities van de International Telecommunication Union 2012 en The Internet Architecture Board 2015.

99 Dutch Data Center Association, p. 6.

100 Internet Society 2015, p. 17. Zie ook Gartner IT Glossary, https://www.gartner.com/it-glossary/Internet-of-things/: 'The Internet of Things (IoT) is the network of physical objects that contain embedded technology to communicate and sense or interact with their internal states or the external environment' (laatst geraadpleegd 27 december 2017).

101 Via: https://en.oxforddictionaries.com/definition/Internet_of_things (laatst geraadpleegd 22 februari 2018).

102 Poudel 2016, p. 999.

het Internet te communiceren. Het World Wide Web betreft slechts een manier om het Internet te gebruiken. De termen Internet en World Wide Web zijn dus niet inwisselbaar. Dit neemt niet weg dat het World Wide Web de primaire wijze is waarop mensen van het Internet gebruik maken. Het World Wide Web wordt gekenmerkt door actief gebruik van het Internet. Door het intypen van zoekopdrachten in een browser, het inloggen op sociale media en het versturen van e-mails worden data gegenereerd en wordt informatie verzonden. Het Internet of Things wordt gekenmerkt door een meer passieve interactie met het Internet. Auto's, huishoudelijke apparaten en ziekenhuisapparatuur verzamelen, versturen en ontvangen data zonder actieve betrokkenheid van gebruikers bij deze interactie met het Internet.[103] Het Internet of Things staat daarmee voor een verandering in de wijze waarop van het Internet gebruik wordt gemaakt. Het verbindt het Internet met de fysieke wereld via talloze sensoren en leidt zo tot een 'zintuiglijk' Internet.[104]

Door de lage kosten, hoge snelheid en alomtegenwoordigheid van het Internet en draadloze datanetwerken is sprake van 'ubiquitous connectivity', waarin alle objecten verbonden kunnen worden met de globale infrastructuur van informatie- en communicatietechnologie.[105] De toegenomen connectiviteit van objecten maakt dat de verzamelde data gedeeld kunnen worden met andere objecten en netwerken. Onder IPv4 (Internet Protocol versie 4) bestond het gevaar dat het aantal IP-adressen opraakte. Met ingebruikname van het IPv6 (Internet Protocol versie 6) is het mogelijk geworden om grote hoeveelheden apparaten van een IP-adres te voorzien. Het risico van een tekort aan IP-adressen doet zich onder IPv6 niet meer voor. De enorme hoeveelheden gegeneerde data worden steeds vaker opgeslagen en verwerkt in de 'Cloud'. Dit betekent dat data niet op één plek (bijvoorbeeld in een *data warehouse*) worden opgeslagen, maar decentraal op verschillende servers op verschillende locaties. Hierdoor kunnen de grote hoeveelheden data die worden verzameld door met het Internet verbonden apparaten eenvoudig en goedkoop worden opgeslagen.[106]

I.3.1.2 'Things'

De 'alledaagse objecten' – de 'Things' in het Internet of Things – hebben gewoonlijk een aantal componenten:[107]

– Een sensor die fysieke stimuli als beweging, hitte, geluid, druk of de nabijheid van personen kan detecteren. Deze waarneming wordt vervolgens omgezet naar een analoog of digitaal signaal, zodat dit leesbaar is voor mensen of computers. Daardoor stellen

103 Idem.
104 Evans 2011, p. 5.
105 International Telecommunication Union 2012, p. 5.
106 Zie uitgebreider over deze 'drivers' van het IoT: The Internet Society 2015, p. 12-14; International Telecommunication Union 2005, p. 9-44.
107 Statrix 2015, p. 12.

sensoren alledaagse objecten bovendien in staat om data te verzamelen, waardoor zij essentieel zijn voor het IoT.[108]
- Mogelijkheden tot het verwerken van de waarnemingen van de sensoren, bijvoorbeeld in de vorm van microprocessoren.
- Een 'actuator' die het object in staat stelt om actie te ondernemen naar aanleiding van de verwerkte waarneming.
- 'Communication abilities' waardoor het object verbinding kan maken met een netwerk of andere apparaten.[109]

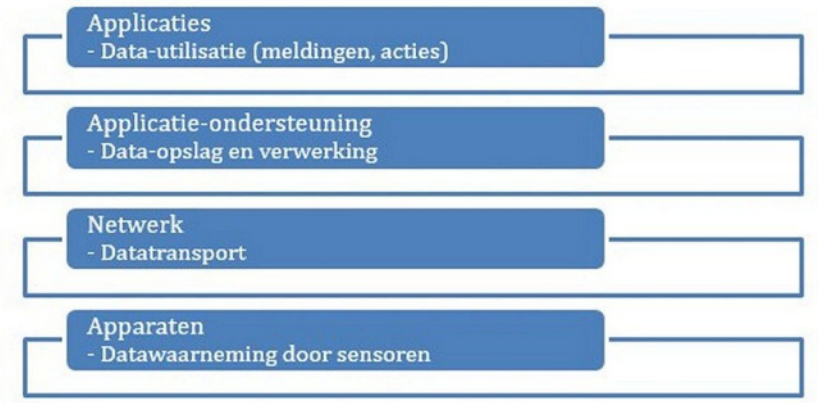
Doordat de chips, sensoren en andere technologieën die gebruikt worden in deze componenten goedkoper, kleiner en energiezuiniger zijn geworden, zijn zij steeds vaker terug te vinden in allerlei objecten. Het is de toenemende aanwezigheid van deze 'sensoren, actuatoren en microprocessoren in, aan en nabij vele alledaagse goederen, objecten en apparaten en de uitwisseling van informatie daartussen en met externe diensten' die een belangrijke rol speelt in de groei van het Internet of Things.[110]

De hoeveelheid IoT-objecten is enorm en varieert van auto's tot huishoudelijke apparaten en van ziekenhuisapparatuur tot industriële toepassingen en zelfs dieren.[111] Al deze 'dingen' zijn in staat om zonder menselijke tussenkomst data te verzamelen en te delen, hetgeen leidt tot een 'hyperconnected world'.[112] IoT-objecten zijn veelal 'heterogeen' van aard. Dit wil zeggen dat zij zijn gemaakt door verschillende fabrikanten, gebaseerd zijn op verschillende soorten hardware en verbonden zijn met verschillende netwerken. Een belangrijke uitdaging voor het Internet of Things is het realiseren van samenwerkingsmogelijkheden en communicatie tussen deze heterogene apparaten en netwerken (interoperabiliteit).[113]

108 International Telecommunication Union 2005, p. 20-27.
109 'The minimum requirement of the devices in the IoT is their support of communication capabilities' – zie International Telecommunication Union 2012, p. 4.
110 Statrix 2015, p. 1.
111 In een beeldend artikel in The Economist werd melding gemaakt van een Nederlands bedrijf dat sensoren in de oren van koeien implanteert om de gezondheid en bewegingen van de dieren te monitoren; The Economist 2010.
112 Internet Society 2015, p. 14.
113 International Telecommunication Union 2012, p. 5.

I.3.2 De architectuur van het Internet of Things

Met de architectuur van het IoT wordt gedoeld op de wijze waarop verschillende IoT apparaten, netwerken en applicaties zich tot elkaar verhouden. Het IoT wordt veelal weergegeven als een vierlagig systeem, dat geïllustreerd wordt in de volgende afbeelding[114]



In de onderste laag ('device layer') bevinden zich met objecten uitgeruste sensoren die data waarnemen en doorgeven. In de netwerklaag ('network services layer') bevindt zich de techniek die zorgt voor het veilige en snelle transport van de data, veelal naar de Cloud. In de Cloud worden data opgeslagen en geanalyseerd ten behoeve van applicatie-ondersteuning. De bovenste laag representeert de applicatielaag ('application services layer'), waarin de geanalyseerde data worden teruggekoppeld naar de gebruiker en/of (automatisch) wordt omgezet in meldingen of acties. Poudel geeft het voorbeeld van een medische IoT-toepassing. Sensoren registreren data over bijvoorbeeld de hartslag van een patiënt. Die data worden via de netwerklaag naar de applicatielaag getransporteerd, waar ze worden opgeslagen en geanalyseerd. De uitkomst van de analyse wordt in de applicatielaag doorgegeven aan de dokter en patiënt die van eventuele afwijkingen op de hoogte worden gesteld.

114 Zie voor soortgelijke afbeeldingen Sethi & Sarangi 2017; Poudel 2016, p. 1001; International Telecommunication Union 2012. De illustratie is een zeer vereenvoudigde versie van de IoT-structuur.

De manier waarop specifieke apparaten met elkaar en met netwerken verbonden zijn, hangt af van door fabrikanten en ontwikkelaars gemaakte keuzes. De onderstaande afbeeldingen illustreren de pluriformiteit van de IoT-architectuur.[115]

Model A: Object-naar-gateway-communicatie
Bij communicatie via een 'gateway' wordt een IoT-object via een zogeheten gateway met het Internet verbonden. Zowel het object als de gateway bevinden zich in de *device layer*. Een voorbeeld van communicatie via een gateway betreft de wijze waarop data van een 'e-health-armband' worden verwerkt. De armband is uitgerust met een sensor die data verzamelt, zoals hartslag of het aantal stappen dat op een dag is gezet. De armband is zelf niet in staat om direct contact te maken het Internet. Daarvoor is de gateway nodig. Een smartphone is een veelgebruikte gateway. De armband en de smartphone zijn met elkaar verbonden via een draadloze verbinding die communicatie op een korte afstand realiseert, zoals Bluetooth. De smartphone, die is uitgerust met een e-health-applicatie, is verbonden met het Internet en in staat om de data door te sturen naar de Cloud, waar de data worden opgeslagen, (verder) verwerkt, geanalyseerd en uiteindelijk teruggekoppeld naar de gebruiker.

Model B: Object-naar-object-communicatie
In het object-naar-object-model zijn IoT-objecten direct met elkaar verbonden. Dit model wordt veel gebruikt bij huishoudelijke IoT-toepassingen. Een voorbeeld is een lamp die is uitgerust met een sensor. Deze sensor neemt de aanwezigheid van personen waar, waarna deze informatie via een netwerk (Wifi, Bluetooth, het Internet etc.) wordt gecommuniceerd naar een lichtschakelaar die de opdracht krijgt om de lamp aan te zetten. De apparaten communiceren met elkaar op een autonome wijze en verzamelen en delen informatie. Zo kan een 'intelligente' woonomgeving worden gecreëerd.[116]

115 Ook hierbij moet worden aangetekend dat het vereenvoudigde weergave betreft van complexe informatietechnologische processen die veelal in samenhang voor komen. De illustraties zijn losjes gebaseerd op de afbeeldingen in International Telecommunication Union 2012, p. 3, Statrix 2015, p. 13 en The Internet Architecture Board 2015.

116 M2M (Machine to Machine) Communication stelt apparaten in staat om met elkaar te communiceren zonder menselijke tussenkomst. M2M wordt veelal gezien als een 'subset' van het IoT. Voor een nader overzicht van de verschillen tussen beiden zie Maple 2017, p. 157-158.

Model C: Object-naar-Cloud-communicatie
Sommige objecten zijn in staat om direct verbinding te maken met de Cloud. Een voorbeeld is de slimme thermostaat die is uitgerust met Internetverbinding. De thermostaat kan data over energieverbruik doorsturen naar een Cloud, waarna de data verder geanalyseerd kunnen worden. In een aanvulling op dit model krijgt gebruiker via een gateway – bijvoorbeeld zijn smartphone – toegang tot de thermostaat, zodat deze op afstand kan worden bestuurd.

I.3.3 Toepassingen

'Het Internet of Things bestaat uit een grote en extreem diverse groep toepassingen.'[117] Slimme woningen, slimme steden en toepassingen in de gezondheidszorg vormen hiervan belangrijke voorbeelden.

Slimme woningen
In een slimme woning (*smart home*) zijn elektronische apparaten en voorzieningen met elkaar en met het Internet verbonden. Voorbeelden van apparaten die met het Internet kunnen worden verbonden zijn huishoudelijke apparaten, verlichting, verwarming, tv's, beveiligingssystemen en camera's. Deze apparaten zijn in staat om onderling informatie uit te wisselen en kunnen op elkaar en op bewoners reageren. Een slimme woning bevordert energiezuinigheid en gebruiksgemak. De mogelijke voorbeelden zijn talloos. Met het afgaan van de wekker, wordt automatisch koffie gezet. De lichten springen aan op het moment dat een bewoner door het huis loopt en de lichtsterkte past zich aan aan het tijdstip van de dag en de stemming van de bewoner. Wanneer de bewoner van werk naar huis vertrekt, begint de oven met voorverwarmen. De koelkast registreert het aantal aanwezige producten in de koelkast en plaatst automatisch een bestelling voor nieuwe boodschappen. Rustge-

117 Statrix 2015, p. 1. Zie ook Weber & Studer 2016, p. 718 en (schematisch) Maple 2017, p. 160-161.

vende muziek wordt aangezet op het moment dat wordt geregistreerd dat de bewoner onrustig is of stress heeft. De thermostaat heeft lerend vermogen en onthoudt door de bewoner gewenste temperaturen op verschillende tijdstippen of bij verschillende stemmingen. Een smart-tv reageert op de stem van de bewoner en schakelt automatisch naar kanalen of films die de bewoner wenst te zien. Kenmerkend voor de slimme woning is dat zij anticipeert op de gebruiker, zich proactief aanpast en diensten op maat levert, soms zelfs voordat de bewoner zich van zijn behoeften bewust is. De apparaten genereren data die door algoritmes wordt geanalyseerd, hetgeen leidt tot een 'eigen wil' van de woning.[118]

Slimme steden

De slimme stad (*smart city*) is een stad die gebruikt maakt van de real-time data die verzameld worden door met sensoren uitgeruste objecten die in verbinding staan met het Internet. Deze gegevens worden tot op heden voornamelijk gebruikt voor het bevorderen van de verkeersstromen in steden en in het veiligheidsdomein.[119] In een slimme stad worden camerагegevens en andere sensoren gebruikt om verkeersstromen – en bijbehoren emissiepatronen – te monitoren en te reguleren. De navigatiesystemen van automobilisten ontvangen informatie over de te rijden route en de beschikbaarheid van parkeerplekken (*smart parking*). Data afkomstig van meldpanelen, alarmsystemen, hekwerkdetectoren en camera's worden ingezet om opstootjes voortijdig te signaleren en grote menigten te controleren. Met behulp van geluidssensoren kan de exacte locatie van pistoolschoten en geweldsmisdrijven worden gedetecteerd.[120] Andere sensoren kunnen de luchtkwaliteit meten en beïnvloeden – samen met de informatie afkomstig van de e-health-armbanden of 'smart watches' van inwoners – het gezondheidsbeleid van gemeenten. Straatlichten passen zich aan aan het tijdstip van de dag, de weersomstandigheden en de nabijheid en gemoedstoestand van personen. De route van vuilniswagens wordt bepaald door sensoren die meten in hoeverre vuilnisbakken en -containers gevuld zijn. Kortom, grote hoeveelheden data kunnen worden gecombineerd en ingezet voor het monitoren van het welzijn en de veiligheid in de slimme stad. De vergaarde kennis kan automatisch leiden tot aanpassingen in de fysieke leefomgeving van burgers.

Gezondheid

In het gezondheidsdomein bestaan hoofdzakelijk drie categorieën IoT-objecten. Objecten die gebruikers dragen (*wearables*), objecten die bij gebruikers worden geïmplanteerd, geïnjecteerd of door hen worden ingeslikt, en niet-draagbare apparaten.[121] Deze objecten kunnen worden ingezet in de gezondheidszorg (in ziekenhuizen of bij patiënten thuis) of

118 Hildebrandt 2010.
119 WRR 2016, p. 62.
120 Internet Society 2015, p. 56.
121 McKinsey 2015, p. 38.

voor persoonlijke gezondheid op niet-medische gronden.[122] Voorbeelden van toepassingen in de gezondheidszorg zijn *wireless diagnostic devices* die de hartslag, temperatuur en ademhaling van patiënten constant meten. Deze apparaten kunnen thuis door patiënten worden gedragen. Waar bijvoorbeeld patiënten met diabetes eerst regelmatig naar het ziekenhuis moesten voor het meten van bloeddruk, suikergehalte en gewicht kan een dokter de waarden nu op afstand monitoren door middel van een armband die deze waarden continu registreert. Mocht de patiënt zijn medicijnen vergeten te nemen, dan wordt dit via een melding aan de patiënt doorgegeven. Op deze wijze kan de gezondheid van patiënten constanter en goedkoper worden gemonitord. Val- en bewegingssensoren voor ouderen in verzorgingstehuizen vormen een ander voorbeeld van controle op afstand. Ook het dragen van 'smart-devices' voor persoonlijke gezondheid komt steeds vaker voor. Dergelijke apparaten, vaak in de vorm van een armband of horloge, meten bijvoorbeeld voedingsinname, hydratatie, beweging, stressniveau en een mogelijk slaaptekort. Als de waarden van een gebruiker onder een bepaald punt zakken, kan de gebruiker hiervan op de hoogte worden gesteld. Op basis van een grote hoeveelheid aan verzamelde data kunnen algoritmes ook bepalen welke activiteiten een persoon moet verrichten om een gezonde levensstijl aan te meten. Dit laat zien dat het IoT in het gezondheidsdomein bij uitstek geschikt is om het gedrag van personen te beïnvloeden.[123] Deze data kan ook voor niet-medische doeleinden worden ingezet. Zo is recent een verband gelegd tussen biologische factoren en crimineel gedrag. Een lage hartslag is bijvoorbeeld een risicofactor die kan indiceren dat er minder cortisol wordt aangemaakt; op zijn beurt houdt een laag cortisolgehalte weer verband met crimineel gedrag.[124] Er is in dit kader voorgesteld om jeugdige delinquenten wearables te laten dragen die voortdurend hartslag, huidgeleiding en ademhaling meten.[125] Voortschrijdende technologische ontwikkelingen maken het mogelijk om de sensoren van het internet of Things dusdanig te verkleinen dat deze ook *in* het menselijk lichaam geplaatst kunnen worden.[126]

I.4 Kunstmatige Intelligentie

Het Latijnse *homo sapiens* staat voor 'wijze mens'. Intelligentie definieert ons mens-zijn. Maar intelligentie is niet voorbehouden aan mensen. Reeds in 1950 stelde de Britse wiskunde

122 Statrix 2015, p. 21.
123 Terry 2016.
124 Comet e.a. 2016, p. 184.
125 Van Hout 2017, p. 1036 wijst hierop.
126 Wanneer de sensoren van het internet of Things dusdanig klein zijn dat deze in het menselijk lichaam geplaatst kunnen worden, wordt gesproken van het 'Internet of nano Things'. Zie Van den Hoven van Genderen 2017, p. 12 en Nayyar, Puri & Le 2017.

Alan Turing de vraag 'Can machines think?'.[127] Deze vraag heeft geleid tot de opkomst van een wetenschappelijke discipline met de naam Kunstmatige Intelligentie (KI) (in het Engels: *Artificial Intelligence* (AI)). KI richt zich niet op begrip van menselijke intelligentie, maar gaat een stap verder: er wordt gestreefd naar het creëren van intelligente artefacten. Al vroeg werden resultaten geboekt door computers die schaak konden spelen en in 1997 in staat bleken om de beste speler ter wereld te verslaan.[128] Ook de winst van IBM's supercomputer Watson van de spelshow Jeopardy in 2011 wordt beschouwd als een mijlpaal in het streven naar Kunstmatige Intelligentie. Watson was in staat om gestelde vragen te interpreteren en op zoek te gaan naar het antwoord in boeken, tijdschriften en encyclopedieën. Intelligentie kan zich uiteraard op meer manieren manifesteren dan het spelen van schaak of deelname aan een spelshow. De veelheid aan uitingen van intelligentie – variërend van denkprocessen tot intelligent gedrag – is een van de redenen waarom de discipline Kunstmatige Intelligentie een enorm toepassingsbereik kent.

I.4.1 Definitie, kenmerken en deelgebieden

I.4.1.1 Definitie

Het definiëren van KI is niet eenvoudig, voornamelijk omdat het niet duidelijk is wat onder intelligentie moet worden verstaan. De mogelijkheid om over intelligentie te beschikken wordt primair aan mensen toegedicht, maar wat menselijke intelligentie inhoudt is niet volledig helder. De definitie van intelligentie wordt daardoor veelal geassocieerd met specifieke uitingsvormen van menselijke intelligentie, zoals het gebruik van taal en leervaardigheid.[129] Deze uitingsvormen zijn niet vastomlijnd en op zichzelf niet altijd eenvoudig te begrijpen. John McCarthy, pionier op het gebied van KI, heeft in lijn met het voorgaande aangegeven dat 'the problem is that we cannot yet characterize in general what kinds of computational procedures we want to call intelligent.'[130]

In hun standaardwerk *Artificial Intelligence: A Modern Approach* beschrijven Russell en Norvig definities die in twee categorieën kunnen worden onderverdeeld.[131] Volgens de definities ziet KI respectievelijk op:

– Menselijk of rationeel denken: apparaten of machines bezitten KI wanneer zij in staat zijn om beslissingen te nemen, problemen op te lossen en te leren.

127 Turing 1950, p. 442.
128 Nilsson 2010; Pandolfini 1997.
129 Scherer 2016, p. 359-360.
130 McCarty 2007, p. 3.
131 Russell & Norvig 2010, p. 1-5.

– Menselijk of rationeel handelen: apparaten of machines bezitten KI wanneer zij in staat zijn om activiteiten uit te voeren die intelligentie zouden vereisen als ze door mensen zouden worden uitgevoerd.

KI richt zich volgens voorgaande definities op artefacten die autonoom opereren, leren, begrijpen, reageren op hun omgeving en zich aanpassen aan veranderingen om zo – in het licht van de omstandigheden – te komen tot 'een zo goed mogelijke uitkomst'.[132]

I.4.1.2 Kenmerken

KI wordt gekenmerkt door een hoge mate van autonomie. KI-toepassingen kunnen complexe taken verrichten, zonder menselijke controle of begeleiding. Het aanverwante controleprobleem van KI bestaat daarin dat de mogelijkheid bestaat dat KI-systemen een dusdanige mate van autonomie bezitten dat menselijke controle ervan niet langer mogelijk is. In het verlengende hiervan ligt het kenmerk dat de acties van KI-systemen niet altijd voorspelbaar zijn. In veel instanties wordt het 'denken' van dergelijke systemen als creatief of 'out-of-the-box' getypeerd, omdat het afwijkt van het menselijke denkpatroon. Een goede illustratie hiervan is het zelflerende C-path-programma, dat ontdekte dat het onderzoeken van het weefsel rondom kankercellen kan leiden tot realistischer prognoses dan het onderzoeken van de kankercellen zelf. Dit ging in tegen het gezonde verstand en destijds heersende medische opvattingen. Dit illustreert dat KI-systemen 'have the capacity to come up with solutions that humans may not have considered, or that they considered and rejected in favor of more intuitively appealing options.'[133] Het C-path-programma laat eveneens zien dat KI nauw verbonden is met data. KI kan worden ingezet ten behoeve van grootschalige data-analyse en is als zodanig nauw verbonden met Big Data.[134]

KI-systemen worden daarnaast gekenmerkt door hun ondoorzichtigheid. Een recent populairwetenschappelijk artikel in *Nature* geeft hiervan een goed voorbeeld.[135] Computerwetenschapper Dean Pomerleau probeerde al in 1991 een zelfrijdende auto te bouwen. Hiertoe installeerde hij een computer en een camera in een speciaal geprepareerde auto en programmeerde hij een algoritme dat de auto zou kunnen besturen. De computer bleek bij verschillende testen in staat om stukken van een route zelf te rijden. Tot de auto aankwam bij een brug en uitweek naar de rechterzijde van de weg; de bestuurder kon ternauwernood het stuur grijpen en de auto naar links manoeuvreren. Terug in het lab probeerde Pomerleau uit te vinden waar de fout in het algoritme zat, maar dit bleek welhaast onmogelijk. 27 jaar later zijn de algoritmes waarop KI gebaseerd is vele malen complexer geworden. De ondoorzichtigheid van KI is navenant toegenomen.

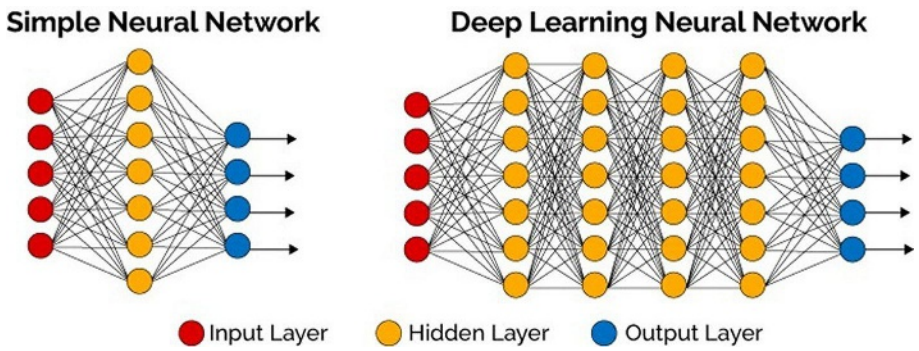
132 Idem en McCarthy 2007.
133 Scherer 2016, p. 365.
134 Government Office for Science 2016, p. 5.
135 Castelbechhi 2016.

I.4.1.3 Deelgebieden

KI kent een veelheid aan deelgebieden, waaronder *natural language processing* (de vaardigheid om gesproken en geschreven taal te verwerken en produceren), *expert systems* (systemen die kennis van een bepaald gebied hebben en die kennis al redenerend op de feiten van een geval kunnen toepassen, bijvoorbeeld in een medische setting)[136] en robotica (het bouwen van machines die programmeerbare taken uit kunnen voeren).[137] De gebieden overlappen en zijn niet altijd van elkaar te onderscheiden, doordat de onderliggende technologieën en algoritmes overeenkomen.[138] De combinatie van ontwikkelingen in al deze deelgebieden heeft ertoe geleid dat KI een breed spectrum aan toepassingen bestrijkt.

Een belangrijk KI-deelgebied houdt zich bezig met technologieën die computers in staat stellen om te leren zonder hiertoe expliciet geprogrammeerd te zijn: *Machine Learning* (ML).[139] ML is gebaseerd op algoritmes die zijn in staat om te leren op basis van eerdere ervaringen, zogenaamde zelflerende algoritmes. Het is dit zelflerende karakter dat ML-algoritmes onderscheidt van 'traditionele' computeralgoritmes. Op basis van ML kunnen computersystemen op basis van eerder uitgevoerde handelingen, anders reageren onder gelijke omstandigheden en zich aanpassen aan nieuwe omstandigheden.[140] De meest geavanceerde toepassing van ML is *Deep Learning*.[141] Deze technologie is gebaseerd op de werking van neurale netwerken die zijn gemodelleerd naar het menselijk brein en de neuronen die zich daarin bevinden. Het dieplerende algoritme voert hierbij een gelaagde analyse uit, waarbij resultaten uit de ene laag worden gebruikt als input voor de analyse van een volgende laag. Zo kunnen complexe, verborgen verbanden in grote datasets worden ontdekt.[142] De onderstaande afbeeldingen illustreren de werking van een eenvoudig en dieplerend neuraal netwerk.[143]

136 Definitie afkomstig van Prakken 2018, p. 271.
137 Zie hierover Muller 2017, par. 2.1.
138 Cerka, Grigiene & Sirbikyte 2017, p. 378.
139 Deze definitie is afkomstig van Samuel 1959. Zie ook Rouse 2017.
140 Cerka, Grigiene & Sirbikyte 2017, p. 377.
141 Forbes 2016.
142 Government Office for Science 2016, p. 7.
143 Deze afbeeldingen zijn afkomstig uit Gill 2017.



Bovenstaande netwerken kunnen bijvoorbeeld worden ingezet voor het proces van gezichtsherkenning. Dit proces kan in een dieplerend neuraal netwerk worden onderverdeeld in verschillende stappen. De 'input' bestaat dan uit de cameraregistratie van een menselijk gezicht. In de eerste stap worden de contouren van het gezicht gedefinieerd. Deze contouren worden beschouwd als een 'verborgen' laag in de afbeelding, omdat deze niet vooraf door een programmeur zijn vastgesteld. De resultaten uit deze laag worden gebruikt voor het analyseren van complexere kenmerken binnen de gedefinieerde contouren, zoals de neus, ogen, oren en mond. In de derde laag worden de verhoudingen tussen de hiervoor omschreven kenmerken gedefinieerd. In de vierde, en laatste, stap worden de resultaten uit de eerdere stappen samengevoegd en vergeleken met informatie afkomstig uit eerdere gezichtsanalyses. De output bestaat uit de herkenning van een specifiek gezicht. In een eenvoudig neuraal netwerk kan het herkenningsproces niet worden opgedeeld in verschillende stappen. Het is daardoor voor een eenvoudig neuraal netwerk ondoenlijk om accuraat gezichten te herkennen.[144]

Zelflerende algoritmes vormen een belangrijke basis om te komen tot *knowledge discovery* in datasets en worden ingezet op een grote hoeveelheid aan terreinen, variërend van fraudeherkenning en het doen van aanbevelingen in online webshops tot het voorspellen van aandelenkoersen. Het zelflerende algoritme is in staat om vele patronen, verbanden en kenmerken te herkennen in grote hoeveelheden data. Het zelflerende karakter schuilt vervolgens in het zelflerende vermogen van het algoritme en – bij dieplerende algoritmes – in de mogelijkheid om gebruik te maken van de neurale netwerken. Eerder herkende patronen worden gebruikt in de data-analyse en het algoritme is in staat zichzelf aan te passen aan eerder gevonden resultaten.

144 Mayer 2015.

ML is nauw verbonden met Big Data-analyse (datamining) en het functioneren van IoT-applicaties. De in paragraaf I.2.1.2 beschreven datamining-technieken vinden hun grondslag veelal in dieplerende algoritmes die zijn ontwikkeld binnen het domein van ML. De processen van patroonherkenning, *profiling*, clustering, associatie en (on)begeleide analyse worden dan ook vaak in de context van ML besproken en behoren niet louter tot de Big Data-context.[145] Big Data stelt dergelijke algoritmes echter wel in staat om hun zelflerende vermogen maximaal te ontplooien. Data-analyse is daarnaast onontbeerlijk voor het adequaat functioneren van IoT-toepassingen. Hieruit volgt dat *Machine Learning* een onmisbare bouwsteen vormt voor de werking van de drie technologieën die de kern vormen van dit onderzoek.

I.4.2 Toepassingen

Veel van de toepassingen van Big Data en het IoT vertonen raakvlakken met KI. Hieronder worden enkele voorbeelden genoemd die nog niet aan bod zijn gekomen in de paragrafen over Big Data en het IoT.

Robotica: Zorgrobots en autonome wapensystemen
Robotica is een discipline die ziet op het bouwen van robots, dat wil zeggen programmeerbare machines die taken uit kunnen voeren. Robots vormen de fysieke manifestatie van het streven naar KI; robotica wordt dan ook wel gezien als een deelgebied van KI.[146] Voorbeelden van deze belichamingen van KI zijn zorgrobots en autonome wapensystemen.

- Zorgrobots voorzien in de zorg van kwetsbare groepen als kinderen, ouderen of gehandicapten. Dergelijke robots worden geproduceerd in meer en minder geavanceerde varianten. Zo is de robot Robear gericht op het verrichten van een enkele handeling: het uit bed tillen van patiënten.[147] Zora de zorgrobot, die in 2016 in Rotterdam werd geïntroduceerd, is in staat om meerdere complexe handelingen te verrichten.[148] Zora heeft vele sensoren in haar hoofd, handen en voeten en beschikt over richtmicrofoons en camera's. KI stelt Zora in staat om te praten, luisteren en autonoom te bewegen en te handelen.
- Autonome wapensystemen (ook wel 'killer robots') zijn KI-gedreven wapens. Dergelijke wapens kunnen worden onderverdeeld in drie categorieën: 'Human-*in*-the-loop'-wapens, waarbij op basis van KI doelen worden geselecteerd die slechts worden aange-

145 Mitchell 1997, p. 1. Zie voor de verschillen Calders & Custers 2013, p. 29. In Russell & Norvig 2010, p. 693-859 wordt de werking van deze algoritmes uitgebreid beschreven.
146 Kool e.a. 2017, p. 16.
147 Kool e.a. 2017, p. 25.
148 'Hallo, ik ben Zora de Zorgrobot', *Algemeen Dagblad* 12 februari 2016, online via: https://www.ad.nl/rotterdam/hallo-ik-ben-zora-de-zorgrobot~a1247f01/ (laatst geraadpleegd 8 januari 2018).

vallen na een menselijk commando (denk aan het inzetten van drones)[149]; 'Human-*on*-the-loop'-wapens, die doelen selecteren en aanvallen onder menselijke controle en 'Human-*out*-of-the-loop'-wapens, die volledig KI-gedreven zijn. In het laatste geval selecteert de robot zelf zijn doel en valt hij aan zonder menselijke tussenkomst of interactie.[150]

Gezichts- en emotieherkenning

Zoals in paragraaf I.4.1.3 is omschreven kunnen dieplerende algoritmes worden ingezet ten behoeve van gezichtsherkenning. Een geavanceerde toepassing van gezichtsherkenning is emotieherkenning. Het bedrijf 'Emotient' ontwerpt bijvoorbeeld software die door middel van patroonherkenning op basis van een gezichtsuitdrukking iemands gemoedstoestand kan herkennen en toekomstig gedrag kan voorspellen.[151] Deze vorm van emotieherkenning kan onder meer worden ingezet voor het analyseren van de houding van personen ten opzichte van een bepaald product of politieke commercial, voor het bepalen van de gemoedstoestand van patiënten of voor psychologisch onderzoek.[152]

Het juridische domein

Jaap van den Herik, hoogleraar Informatica en recht, sprak in 1991 zijn oratie uit met de titel 'Kunnen computers rechtspreken?'.[153] In het licht van de snelheid van technologische ontwikkelingen lijkt een bevestigend antwoord op deze vraag onvermijdelijk.[154] Algoritmes die zijn ontwikkeld binnen de domeinen *natural language processing* en *machine learning* kunnen met een grote mate van zekerheid rechterlijke uitspraken voorspellen of kunnen worden ingezet om de slaagkans van de stap naar de rechter te voorspellen.[155] De voorzitter van de Raad voor de Rechtspraak gaf recent aan dat eenvoudige zaken in de toekomst geautomatiseerd afgedaan kunnen worden.[156]

149 *Handelingen II* 2013-2014, 30806, nr. 24.
150 Human Rights Watch 2012.
151 Business Insider 2016.
152 Zie uitgebreider voor technologische achtergronden Miyakoshi, Yoshihiro en Kato 2011.
153 Van den Herik 1991.
154 Zie een citaat van Van den Herik: 'Uiteindelijk kan de computer iedere rechter vervangen, denkt hij. 'Daar ben ik honderd procent van overtuigd. Juristen hebben de kracht van zelflerende programma's nog niet in de gaten. Dus zeggen ze: het mag niet. Maar waarom zou je het willen tegenhouden?', 'Is een robot als rechter daadwerkelijk objectiever. Het vonnis van de machine', *De Volkskrant* 14 oktober 2017, online via: https://www.volkskrant.nl/tech/is-een-robot-als-rechter-daadwerkelijk-objectiever~a4521674/ (laatst geraadpleegd 9 januari 2018).
155 Respectievelijk Aletras e.a. 2016 en Van Est & Gerritsen 2017, p. 42.
156 *De Volkskrant* 2017.

I.5 Gemeenschappelijke deler: slimme algoritmes

Big Data, Internet of Things en Kunstmatige Intelligentie zijn samenhangende technologieën. Het IoT draagt bij aan de explosie van data. Dit maakt dat het IoT en Big Data onlosmakelijk met elkaar zijn verbonden.[157] Het analyseren van grote hoeveelheden uiteenlopende real-time-data (Big Data) is een complexe aangelegenheid die mede mogelijk wordt gemaakt door datamining en KI, waarbij het leren door machines door middel van neurale netwerken essentieel is.[158] Algoritmes vormen daarbij de cruciale verbindende factor tussen Big Data, IoT en KI.

- De aanwezigheid van grote hoeveelheden gegevens (Big Data) maakt dat het zoeken naar relevante verbanden en patronen neerkomt op het vinden van een naald in een hooiberg. Algoritmes vormen de oplossing voor deze uitdaging en maken datamining en profilering mogelijk. Zij helpen immers om zinvolle informatie te destilleren uit de grote hoeveelheden data die mensen en apparaten genereren.[159]
- Voor het functioneren van het IoT is de analyse van de grote hoeveelheid verzamelde data en snelle terugkoppeling hiervan aan apparaten of gebruikers essentieel.[160] Algoritmes staan centraal in dit proces. Algoritmes maken het mogelijk om de door sensoren geregistreerde informatie te verwerken en te analyseren op een zodanige manier dat die bruikbaar wordt voor een applicatie. De voornaamste algoritmische uitdaging voor het IoT is gelegen in de snelle terugkoppeling van de resultaten van data-analyse, zodat IoT apparaten in staat zijn om direct - en waar mogelijk proactief - te reageren op veranderingen in de omgeving. Daardoor kan het IoT real-time interveniëren in de levens van mensen.
- Kunstmatige Intelligentie en *Machine Learning* maken gebruik van algoritmes die apparaten in staat stellen zicht intelligent te gedragen en zelf te leren.[161]

Het functioneren van de drie technologieën hangt dus af van de algoritmes die worden gebruikt. Hieronder wordt – in aanvulling op hetgeen in dit hoofdstuk reeds over algoritmes is geschreven – nader ingegaan op de definitie en kenmerken van (slimme) algoritmes.

I.5.1 'Domme' en 'slimme' algoritmes

Algoritmes bestaan uit een set instructies die worden ingezet voor het oplossen van bepaalde problemen. Deze set instructies is in staat om inputdata om te zetten naar outputdata ten

157 Zie in deze trant WRR 2016, p. 37; De Koning 2016; Poudel 2016, p. 1005-1006.
158 Zie voor een soortgelijke analyse UK Information Commissioner 2017, p. 8.
159 Vedder & Naudts 2017, p. 207; Colonna 2013, p. 330.
160 Poudel 2016, p. 1007-1008.
161 Russel & Norvig 2010; Vedder & Naudts 2017, p. 209.

behoeve van het oplossen van het probleem.[162] In een eenvoudig voorbeeld wordt een algoritme gebruikt om het hoogste getal in een grote lijst met getallen te vinden. De lijst met getallen vormt daarbij de inputdata. Vervolgens wordt de volgende set instructies gedefinieerd:

1) het eerste nummer in de lijst is het hoogste getal (*max*);
2) vergelijk ieder nummer in de lijst (*x*), met *max*; als *x* hoger is, verander *x* dan naar *max*.

De *output* van het algoritme is kennis en vormt de oplossing voor het gegeven probleem. Zo beschouwd zijn algoritmes niet meer dan een recept; een precieze set aan instructies.[163] Voor de het genereren van de output van algoritmes (de uitvoering) worden vaak computers gebruikt. Computers zijn 'algoritme-machines', die zijn gemodelleerd om data op te slaan, hier wiskundige formules op los te laten en nieuwe informatie als *output* te leveren.[164] In het gegeven voorbeeld wordt gebruik gemaakt van een IFTTT-algoritme (*If This Then That*-algoritme). Een dergelijk algoritme bestaat uit een vooraf gedefinieerde set aan instructies, die een 'als-dan' structuur hebben. Het algoritme van een thermostaat kan gebruik maken van een IFTTT-structuur. 'Als' de temperatuur in een huis onder een bepaalde temperatuur zakt, 'dan' wordt de verwarming aangezet. Dergelijke algoritmes zijn 'dom', in die zin dat ze niet zelf leren. De werking van het algoritme bestaat alleen daarin dat de IFTTT-instructie wordt uitgevoerd. Door technologische ontwikkelingen, met name op het terrein van *Machine Learning*, zijn algoritmes in toenemende staat om te leren op basis van de kennis die zij zelf genereren. Dergelijke algoritmes kunnen zich automatisch aanpassen aan eerder behaalde resultaten. Gedane observaties worden onderdeel gemaakt van de 'trainingsdata' van het algoritmes, op basis waarvan het algoritme zichzelf aanpast, verfijnt en ontwikkelt. Hillebrandt geeft aan dat zowel 'domme' als 'slimme' algoritmes kunnen worden ingezet ten behoeve van besluitvorming.[165] De in dit hoofdstuk beschreven algoritmes zijn veelal slimme algoritmes, omdat deze – beter dan hun niet-zelflerende tegenhangers – bij uitstek geschikt zijn voor het verrichten van complexe (voorspellende) analyses.

I.5.2 Algoritmes als ondoorzichtige, niet-neutrale menselijke constructen

Algoritmes kunnen worden gekarakteriseerd als ondoorzichtige en niet-neutrale menselijke constructen:

– Mensen zijn verantwoordelijk voor het programmeren en (waar nodig) trainen van algoritmes. Algoritmes zijn daarmee primair menselijke creaties. Het belang van de

162 Zie o.a. WRR 2016, p. 21 en Diakopoulos 2014, p. 400.
163 Hildebrandt 2016c, p. 56.
164 Gillespie 2014, p. 167.
165 Hillebrandt 2016, p. 55-56.

door mensen gemaakte keuzes in de ontwerpfase kan nauwelijks worden onderschat, onder meer omdat deze keuzes doorwerken in de analyse en de uiteindelijke uitkomst van de analyse.[166]

- De uitspraak 'Technology is neither good nor bad; nor is it neutral'[167] geldt ook voor algoritmes. Ondanks de 'belofte' van algoritmische objectiviteit kunnen algoritmes op vele manieren blijk geven van subjectiviteit.[168] Doordat algoritmes menselijke constructen zijn, kunnen de vooroordelen en waarden van programmeurs of opdrachtgevers van programmeurs worden ingebed in algoritmes.[169] Zo kunnen de algoritmes die worden ingezet in het kader van het prioriteren van zoekresultaten of nieuwsberichten, waarden bevatten die politiek gekleurd of anderszins niet-neutraal zijn. De oefendata waarmee een zelflerend algoritme wordt getraind, kunnen eveneens *biases* bevatten die bepalend zijn voor de uitkomsten van het algoritme.
- De ondoorzichtigheid van slimme algoritmes hangt nauw samen met hun complexiteit. Algoritmes zijn complex op twee met elkaar verbonden manieren: technologisch en contextueel.[170] Algoritmes worden door programmeurs vastgelegd in programmeertaal, waarna deze 'vertaald' worden in een binaire sequentie (nullen en enen) die een computer kan begrijpen. Om een dergelijke technisch construct goed te begrijpen is kennis van de technologische werking van het algoritme onontbeerlijk. De complexiteit van een algoritme is echter niet alleen gelegen in het algoritme als zodanig, maar ook in de specifieke context waarin het algoritme opereert. Algoritmes worden immers gekoppeld aan datasets.[171] Deze datasets kunnen bestaan uit gevarieerde data, die vooraf geclassificeerd en geprepareerd zijn voor data-analyse. Het algoritme wordt bovendien aan een dataset gekoppeld met een bepaalde opdracht, die moet worden uitgevoerd in de context van de specifieke dataset. Wanneer slimme algoritmes in een Big Data-setting worden ingezet, blijken zelfs computerexperts niet altijd in staat om de werking en uitkomst van een algoritme te begrijpen. Deze complexiteit wordt versterkt wanneer algoritmes met elkaar zijn verbonden, bijvoorbeeld als een algoritme voortbouwt op de uitkomsten van een ander algoritme. Algoritmes worden hierdoor vaak gezien als een 'black box':[172] de input en output van het algoritme zijn bekend, maar hoe het tussenliggende proces functioneert is lastig te doorgronden.[173] Dit geldt vooral voor slimme algoritmes.[174] Deze complexiteit en de daarmee samenhangende ondoorzichtigheid

166 Diakopoulos 2014, p. 402.
167 Kranzberg 1986, p. 547.
168 Gillespie 2014, p. 179.
169 Citron & Pasquale 2014, p. 4; Vedder & Naudts 2017, p. 208.
170 Vedder & Naudts 2017, p. 208-210.
171 Gillespie 2014, p. 169.
172 Pasquale 2015.
173 Rouvroy 2012, p. 12.
174 Hildebrandt 2016c, p. 58.

maken het moeilijk om het besluitvormingsproces van het algoritme en (in het licht hiervan) de uitkomsten ervan te beoordelen. De uitkomst van een algoritme is hierdoor (*ex ante*) lastig te voorspellen en (*ex post*) lastig uit te leggen.[175] Bovendien zijn algoritmes vaak geheim. Om (commerciële of veiligheids-) redenen kiezen bedrijven en overheden ervoor om de algoritmes die ten grondslag liggen aan besluitvorming niet openbaar te maken. Als de Belastingdienst bijvoorbeeld inzage zou geven in het algoritme dat gebruikt wordt om belastingfraude op te sporen in belastingaangiftes, zouden belastingplichtigen hun aangifte hierop kunnen afstemmen.[176]

– In het verlengde van het voorgaande ligt dat dat de *output* van een algoritme fouten kan bevatten en met enige onzekerheid wordt omgeven. De 'oriëntatie op correlatie' maakt dat algoritmes die worden ingezet bij data-analyse geen inzicht bieden in causale verbanden, maar slechts wijzen op (mogelijk nuttige) correlaties. De oefendata van classificatie-algoritmes kan fouten bevatten en het opstellen van niet-distributieve groepsprofielen is per definitie onnauwkeurig, omdat de kenmerken van een bepaalde groep niet per definitie op alle leden van deze groep van toepassing zijn. Als onnadenkend of onkritisch wordt omgegaan met *outcomes* van algoritmes, kan dit leiden tot fouten in publieke en private besluitvorming.

I.5.3 Algoritmische alomtegenwoordigheid

Veel beslissingen die voorheen door mensen werden genomen, worden nu algoritmisch bepaald. Algoritmische besluitvorming is inmiddels alomtegenwoordig.[177] In dit hoofdstuk zijn vele illustraties de revue gepasseerd, variërend van de opsporing van strafbare feiten, nieuwsvoorziening op sociale media, het toekennen van leningen en slimme huizen tot verkiezingsstrategieën en gezondheidszorg. Slimme algoritmes zijn in toenemende mate sturend voor het handelen van overheid, bedrijven en particulieren. Dit is met name duidelijk waar sprake is van automatisch-algoritmische besluitvorming, zonder enige vorm van menselijke tussenkomst. Duidelijke voorbeelden hiervan zijn de algoritmes die Facebook gebruikt voor het samenstellen van de tijdlijn van zijn gebruikers. Maar ook waar sprake is van semi-automatische besluitvorming is de invloed van algoritmes groot. Als de mens een besluit neemt op basis van een algoritmisch voorbereide beslissing, is er veelal sprake van automatische goedkeuring, omdat mensen de tijd, vaardigheden en het inzicht in het functioneren van het algoritme ontberen om een zelfstandig oordeel te vormen. Zo zal een bankmedewerker niet eenvoudig afwijken van de uitkomst van een kredietwaardigheidscheck door een algoritme. Hierdoor is het onderscheid tussen automatische en semi-

175 Wagner 2017, p. 5.
176 Kroll e.a. 2017, p. 657-658.
177 Kroll 2017, p. 636; Vedder & Naudts 2017, p. 207.

automatische besluitvorming onscherp.[178] Algoritme-gedreven besluitvorming heeft een grote impact op het dagelijks leven van mensen. Daarmee komen ook de fundamentele rechten van mensen in het geding. In het volgende hoofdstuk worden de sets van grondrechten uiteengezet die in dit kader van groot belang zijn; hoofdstuk III gaat vervolgens in op de specifieke bedreigingen voor die grondrechten die uitgaan van algoritme-gedreven besluitvorming.

178 Wagner 2017, p. 6.

II Het Nederlands grondrechtelijk kader

II.1 Privacyrechten

II.1.1 Inleiding

In het recht speelt het recht op privacy – ook wel aangeduid als het recht op privéleven of de eerbiediging van de persoonlijke levenssfeer – een voorname rol. Het recht houdt nauw verband met de noties van menselijke waardigheid en persoonlijke autonomie. Menselijke waardigheid ligt als notie ten grondslag aan alle grondrechten. Het enkele zijn van mens gaat gepaard met een bepaalde waardigheid, die een beschermingsniveau ten opzichte van de overheid en derden garandeert, bijvoorbeeld als het gaat om fysieke en geestelijke integriteit. Persoonlijke autonomie ligt in het verlengde van menselijke waardigheid. Een mens moet vrijelijk keuzes kunnen maken en uiteindelijk grotendeels zelf kunnen bepalen hoe hij zijn leven inricht. Het recht op privacy is met deze beide noties nauw verbonden. In oudere literatuur wordt dit recht veelal omschreven als het recht om met rust te worden gelaten.[179] Moderner is de formulering dat het individu het recht heeft om 'zichzelf' te zijn en te doen en laten wat hij wil, zonder bemoeienis van de overheid of derden. Zo gaf in de jaren zestig de toenmalige minister van Binnenlandse Zaken de volgende definitie van de persoonlijke levenssfeer: '(…) de reeks van situaties, waarin de mens, al dan niet in zelf gekozen gemeenschap, onbevangen zichzelf wil zijn.'[180] Dit recht om zichzelf te zijn heeft iemand zowel thuis, anders gezegd in het privédomein, als in de publieke of digitale ruimte.[181] Het lastige van het recht is tegelijkertijd dat het moeilijk te definiëren valt. De regering stelde naar aanleiding van de definitie van de minister in ieder geval dat deze definitie niet uitputtend moest worden geacht; het nieuwe art. 10 Grondwet (persoonlijke levenssfeer) zou in wetgeving en rechtspraak nadere omlijning moeten vinden.[182]

In de afgelopen decennia heeft die omlijning daadwerkelijk plaatsgevonden, met name door (semi-)rechterlijke instanties (EHRM, Europese Hof van Justitie, Human Rights Committee en Nederlandse gerechten). Zij hebben dat niet alleen gedaan aan de hand van art. 10 Gw, maar ook aan de hand van equivalente verdragsbepalingen, in het bijzonder

179 Een klassieker in dit verband: Warren & Brandeis 1890, p. 193-220.
180 *Kamerstukken II* 1967/68, 9419, nr. 3, p. 3.
181 Zie uitgebreid ook Koops e.a. 2017.
182 *Kamerstukken II* 1975/76, 13782, nr. 3, p. 41.

art. 8 EVRM, art. 7 Hv en art. 17 IVBPR. Deze bepalingen en de rechtspraak daarover staan in deze paragraaf dan ook centraal.

Belangrijk is daarnaast dat een nauw met persoonlijke autonomie en individuele vrijheid verwant recht een aparte plaats heeft gekregen in de relevante grondrechtencodificaties, namelijk de gewetensvrijheid en de vrijheid om een mening te koesteren.[183] Meestal worden deze vrijheden beschouwd als onderdelen van de vrijheid van godsdienst respectievelijk de vrijheid van meningsuiting. Zij kunnen echter worden onderscheiden van de godsdienstvrijheid en de vrijheid van meningsuiting zoals die meestal wordt beschouwd. Het gaat hierbij immers niet om het *uiten* van bepaalde opvattingen (bijvoorbeeld door religieuze samenkomsten of door publicatie), maar om het *hebben* van die opvattingen. Daarmee zijn deze rechten sterk intern, naar het wezen van het individu gericht, en niet zozeer naar de buitenwereld. Niet voor niets wordt de gewetensvrijheid dan ook gezien als het *forum internum*, terwijl religieuze uitingen worden beschouwd als het *forum externum*.[184] De relatie tussen dit *forum internum* en de privacy is daardoor bijzonder sterk, zodat het voor de hand ligt om dit onderwerp in deze paragraaf te behandelen en niet in de paragraaf over vrijheidsrechten (paragraaf II.3).[185]

In het hiernavolgende zal een beknopt overzicht worden gegeven van de diverse aspecten van het recht op privacy en van het *forum internum*. Daarbij dient de kanttekening te worden geplaatst dat ook het recht op de bescherming van persoonsgegevens een belangrijk recht is dat voortvloeit uit het meer algemene recht op privacy. Zoals in de inleiding op dit onderzoek uiteengezet, zal dit recht hier echter buiten beschouwing wordt gelaten. Gelet op de onderlinge verbondenheid van de hierboven al besproken noties van privacy, persoonlijke autonomie en menselijke waardigheid, en de complexiteit van die drie noties, zal worden begonnen met een korte duiding van deze begrippen (paragraaf II.1.2). Vervolgens wordt ingegaan op de codificatie van het recht op privacy en van het *forum internum* (paragraaf II.1.3). Nadat bijzondere aandacht is besteed aan de grondwettelijke codificaties (paragraaf II.1.4), wordt vervolgens een overzicht gegeven van de manier waarop in vooral de Europese rechtspraak verder invulling aan de privacyrechten is gegeven (paragraaf II.1.5).

183 Zie over de vrijheid van geweten tevens Vermeulen 1989.

184 Zie nader over deze terminologie o.m. Vermeulen & Van Roosmalen 2018; Evans 2001, p. 72.

185 Vgl. Evans 2001, p. 72, die uitlegt dat het bij het *forum internum* in wezen gaat om 'the primacy of the private sphere'.

II.1.2 Menselijke waardigheid, persoonlijke autonomie, zelfbeschikking en het persoonlijkheidsrecht

Menselijke waardigheid, persoonlijke autonomie en zelfbeschikking

In een voorstudie voor de Staatscommissie Grondwet 2010 hebben Brems en Vrielink onderzocht welke betekenis het begrip menselijke waardigheid heeft en of en in welke vorm een grondwettelijke verankering van dit begrip gestalte zou kunnen krijgen.[186] Zij onderscheiden drie functies van een recht of principe van menselijke waardigheid. In de eerste plaats zien zij dit als richtinggevend principe bij de interpretatie van specifieke grondrechten. In de tweede plaats kan menselijke waardigheid worden gezien als autonoom grondrecht en in de derde plaats als element in de afbakening van toegelaten beperkingen op grondrechten. Zij concluderen dat inhoudelijk het recht of principe van menselijke waardigheid in verschillende contexten gehanteerd kan worden en dan in het bijzonder in de voornaamste 'categorieën van mensenrechtenbescherming zoals: de fysieke en psychologische, integriteit, individuele autonomie, materiële levensomstandigheden en gelijkheid'.[187]

In een aantal landen is de menselijke waardigheid inderdaad als afzonderlijk autonoom grondrecht gecodificeerd, maar in de rechtspraak in die landen blijkt dat het veelal wordt gebruikt als 'steunrecht' voor de interpretatie van andere grondrechten.[188] Een voorbeeld daarvan is te vinden in de Duitse Grondwet, waar de menselijke waardigheid prominent is te vinden in art. 1. In Duitsland heeft dit echter tot op heden geen zelfstandige jurisprudentie opgeleverd, maar wordt de bepaling wel gebruikt om andere grondrechten nader in te vullen.[189] Ook wordt de menselijke waardigheid in dit soort systemen soms als 'beperkingsbeperker' gebruikt – grondrechten mogen niet zodanig ver worden ingeperkt dat de menselijke waardigheid in het gedrang lijkt te komen.[190]

Deze diversiteit van betekenissen en functies van de notie van menselijke waardigheid komt ook tot uitdrukking in diverse internationale, ook voor Nederland relevante, verdragen. In de preambule van het VN-Handvest wordt de 'waardigheid van de mens' bijvoorbeeld gehanteerd als een van de grondslagen en na te streven beginselen van de VN. In de UVRM wordt het beginsel op vier plaatsen genoemd: in de preambule (twee keer), in art. 1, art. 22 en art. 23, derde lid. Meer concreet bepaalt art. 1 Hv dat de menselijke waardigheid onschendbaar is en dat zij moet worden geëerbiedigd en beschermd. Ook in deze bepaling is menselijke waardigheid weliswaar expliciet als subjectief grondrecht geformuleerd,[191]

186 Brems & Vrielink 2010.
187 Brems & Vrielink 2010.
188 Vgl. Janssen 2003.
189 Zie ook hieronder met betrekking tot het algemeen persoonlijkheidsrecht.
190 Zie in het bijzonder Leijten 2015.
191 Zie daarvoor de toelichtingen bij art. 1 Hv.

maar de praktijk wijst tot nu toe uit dat het grondrecht vooral een interpretatieve en 'beperkingsbeperkende' functie heeft.[192] Opmerkelijk genoeg is een recht op menselijke waardigheid niet expliciet terug te vinden in het EVRM; de notie wordt zelfs niet genoemd in de preambule.[193] Niettemin heeft het EHRM altijd aangenomen dat menselijke waardigheid een belangrijk beginsel is dat ten grondslag ligt aan het EVRM als geheel: 'The very essence of the Convention is respect for human dignity and human freedom'.[194] Als zodanig is menselijke waardigheid ook voor het EHRM een belangrijke 'hulpwaarde' bij het interpreteren van grondrechten.[195]

Hiervoor is al aangegeven dat persoonlijke autonomie vaak wordt gezien als onderdeel van de menselijke waardigheid of als een verlengstuk ervan. Het individu dient in een rechtsstaat ruimte te hebben om zijn eigen afwegingen te maken; waar hij woont, hoe hij leeft, welk geloof hij wel of niet aanhangt, welke opleiding hij kiest, welke baan hij accepteert, of welke partner(s) hij zijn leven wil delen, enzovoorts. Persoonlijke autonomie is een iets specifiekere notie dan menselijke waardigheid en is nauwer gelieerd aan het recht op privéleven. Ook dit recht is in veel gevallen niet expliciet gecodificeerd. Art. 1 Hv noemt het niet expliciet en ook in het EVRM is persoonlijke autonomie niet als afzonderlijk grondrecht vastgelegd. Het EHRM noemt persoonlijke autonomie echter wel als richtinggevend principe bij de interpretatie van EVRM-rechten: 'Although no previous case has established as such any right to self-determination as being contained in Article 8 of the Convention, the Court considers that the notion of personal autonomy is an important principle underlying the interpretation of its guarantees.'[196] Bovendien heeft het EHRM in een beperkt aantal gevallen het recht op persoonlijke autonomie expliciet geaccepteerd als volwaardig subjectief grondrecht, dat wordt beschermd door het in art. 8 EVRM vastgelegde

192 Zie nader Greer, Gerards & Slowe 2018, p. 328. Zie voor voorbeelden van de interpretatieve functie bijv. HvJ EU 18 oktober 2011, zaak C-34/10, ECLI:EU:C:2011:669 (*Brüstle*), *EHRC* 2012/54 m.nt. F.M. Fleurke, *NTM-NJCM-Bull.* 2012, p. 242 m.nt. B. van Beers; HvJ 5 april 2016, gev. zaken C-404/15 en C-659/15 PPU, ECLI:EU:C:2016:198 (*Aranyosi en Căldăraru*), *EHRC* 2016/157 m.nt. H. van der Wilt, par. 85; de 'beperkingsbegrenzende' rol komt vooral tot uitdrukking in de toelichtingen bij art. 1 Hv.

193 Alleen in de preambule bij Protocol 13, inzake afschaffing van de doodstraf, is de notie expliciet terug te vinden.

194 EHRM 29 april 2002, nr. 2346/02, ECLI:CE:ECHR:2002:0429JUD000234602 (*Pretty t. het Verenigd Koninkrijk*), *EHRC* 2002/47 m.nt. J.H. Gerards & H.L. Janssen, *NJ* 2004/543 m.nt. E.A. Alkema, *NJCM-Bull.* 2002, p. 910 m.nt. B.E.P. Myjer, par. 64.

195 Gerards 2011b, p. 45.

196 EHRM 29 april 2002, nr. 2346/02, ECLI:CE:ECHR:2002:0429JUD000234602 (*Pretty t. het Verenigd Koninkrijk*), *EHRC* 2002/47 m.nt. J.H. Gerards & H.L. Janssen, *NJ* 2004/543 m.nt. E.A. Alkema, *NJCM-Bull.* 2002, p. 910 m.nt. B.E.P. Myjer, par. 61. Zie verder uitgebreid Gerards, Koffeman & Hendriks 2013, p. 29 e.v.

recht op respect voor het privéleven.[197] 'Privéleven' omvat op die manier ook het recht op persoonlijke autonomie.[198]

Aangenomen kan daarmee worden dat zowel de notie van menselijke waardigheid als die van persoonlijke autonomie fundamentele beginselen zijn die de uitleg van andere grondrechten kunnen informeren en kunnen kleuren. Bovendien kunnen zij helpen te bepalen hoe ver beperkingen van de uitoefening van andere grondrechten kunnen reiken. De zelfstandige betekenis van de beide noties is echter beperkt, in die zin dat het moeilijk is om rechtstreeks een van deze beginselen als grondrecht in te roepen. Meer concrete grondrechten, zoals het recht op privacy of de vrijheid om een mening te koesteren, zijn daarmee voor de praktijk relevanter. In het navolgende wordt daarom vooral aandacht besteed aan de verschillende aspecten van het recht op privacy en wordt in mindere mate ingegaan op menselijke waardigheid en persoonlijke autonomie.

Algemeen persoonlijkheidsrecht

In het kader van de bespreking van algemene en aan privacy gerelateerde noties is het ten slotte nog nuttig om te wijzen op het algemeen persoonlijkheidsrecht.[199] In de jaren negentig van de vorige eeuw heeft de Hoge Raad in een beperkt aantal zaken gewezen op dit recht. Als eerste betrof dat het arrest *Valkenhorst* uit 1994 waarin een vrouw inzage wilde krijgen in de archieven van een voormalig opvanghuis voor ongetrouwde moeders (Valkenhorst).[200] In die archieven lagen de gegevens besloten van haar biologische vader waarnaar zij op zoek was. Het bestuur van Valkenhorst weigerde inzage en deed een beroep op zijn geheimhoudingsplicht, mede gebaseerd op het zwijgen van de moeder. De Hoge Raad oordeelde dat de dochter inzage diende te hebben in haar afstammingsgegevens op grond van het algemeen persoonlijkheidsrecht dat ten grondslag ligt aan grondrechten als het recht op respect voor respect voor het privéleven, het recht op vrijheid van gedachte, geweten en godsdienst en het recht op vrijheid van meningsuiting. De Hoge Raad kwam met deze grondslag op voorspraak van Advocaat-Generaal Koopmans. De AG haalde zijn inspiratie hiervoor uit de Duitse constitutionele rechtspraak, waarin het algemeen persoonlijkheidsrecht door het Duitse federale constitutionele hof is afgeleid uit art. 1 (menselijke waardigheid) en art. 2 (persoonlijke ontplooiing) van de Duitse Grondwet (Grundgesetz). Van belang is hierbij wel op te merken dat in het Grundgesetz niet een expliciet grondrecht op persoonlijke levenssfeer is gecodificeerd en ook dit recht, naast onder andere het recht

197 Vgl. Gerards, Koffeman & Hendriks 2013, p. 31.

198 Zie bijv. EHRM 7 maart 2006, nr. 6339/05, ECLI:CE:ECHR:2007:0410JUD000633905 (*Evans t. het Verenigd Koninkrijk*), *NJ* 2007/459 m.nt. J. de Boer, *EHRC* 2006/47 m.nt. E. Brems, par. 57.

199 Zie nader over dit onderwerp: Nehmelman 2002; Janssen 2003.

200 HR 15 april 1994, *NJ* 1994/608 (*Valkenhorst*).

op de kennis van de eigen afstamming, valt onder het (Duitse) algemeen persoonlijkheidsrecht.

De andere, eveneens civiele zaak waarin het algemeen persoonlijkheidsrecht een prominente betekenis had, is het arrest *Het Parool*.[201] In deze zaak stond de vraag centraal of het dagblad *Het Parool* onrechtmatig had gehandeld na het publiceren van een artikel in het dagblad over de bekende cineast Louis van Gasteren inzake zijn oorlogsverleden. Het Parool stelde dat Van Gasteren in de oorlog een onderduiker (Oettinger) had geliquideerd voor geldelijk eigen gewin. Van Gasteren stelde daarentegen dat hij dat had gedaan als verzetsdaad aangezien de onderduiker een groot risico zou vormen vanwege klikken. Bovendien stelde Van Gasteren dat hij kort na deze daad was veroordeeld voor doodslag en dat uiteindelijk gratie was verleend. Opvallend in deze zaak is derhalve dat Van Gasteren de daad had gepleegd en bovendien rechtmatig was veroordeeld. Daar zat dan ook de onrechtmatigheid niet in; de kern van zijn betoog was dat het oprakelen van dit verleden een onrechtmatigde daad was vanwege het beledigen van zijn persoon. De Hoge Raad oordeelde genuanceerd en overwoog:

> 'Daarbij verdient aantekening dat in dit geval niet louter de goede naam van Van Gasteren in het geding is, maar tevens en zelfs in de eerste plaats diens – uit zijn algemene persoonlijkheidsrecht af te leiden – recht om niet, méér dan veertig jaar nadat hij voor het ombrengen van Oettinger werd veroordeeld, zijn straf ter zake had ondergaan en voor het overige gratie had gekregen, in het openbaar wederom met deze – op jeugdige leeftijd, onder oorlogsomstandigheden begane – daad te worden geconfronteerd, en dat nog wel in de vorm van de zowel grievende en onterende beschuldiging dat het daarbij, anders dan in het strafvonnis was aangenomen, ging om roofmoord.'

Het algemeen persoonlijkheidsrecht is na het *Parool*-arrest slechts sporadisch toegepast in de Nederlandse rechtspraak. Tot op heden is dat ook nooit meer op een zo indringende wijze gebeurd als in het *Valkenhorst*- en *Het Parool*-arrest. Niettemin gaat het hier om een potentieel belangrijk fundamenteel recht, dat meerwaarde kan hebben voor discussies over de impact van nieuwe technologieën. Het algemeen persoonlijkheidsrecht verenigt immers op een waardevolle manier elementen van privacy, integriteit, menselijke waardigheid en persoonlijke autonomie. Het is dan ook niet verbazend dat de interpretatie van het recht op persoonlijke levenssfeer (art. 10, eerste lid Gw) en de equivalenten daarvan zoals vervat in art. 8 EVRM, art. 7 Hv en art. 17 IVBPR – waarover hierna meer – in de afgelopen jaren zo zijn geëvalueerd dat voorzichtig kan worden geconcludeerd dat veel toepassingen van

201 HR 6 januari 1995, *NJ* 1995/422 m.nt. E.J. Dommering (*Parool*).

deze rechten overeenkomen met de toepassing van het algemeen persoonlijkheidsrecht zoals hierboven omschreven.[202]

II.1.3 Het recht op privacy en het forum internum – codificaties

Verschillende aspecten van het recht op privacy en de hiervoor omschreven, daaraan nauw verwante noties worden beschermd in art. 10-13 van de Nederlandse Grondwet, in art. 8 EVRM, in art. 7 EU-Grondrechtenhandvest en in art. 17 IVBPR. Tussen deze bepalingen bestaat aanzienlijke overlap. Art. 7 Hv is niet voor niets aangemerkt als een 'corresponderende bepaling' voor art. 8 EVRM, wat betekent dat de Handvestbepaling dezelfde inhoud en reikwijdte heeft als de EVRM-bepaling.[203] Ook art. 17 IVBPR heeft in grote lijnen dezelfde inhoud als de EVRM- en Handvestbepalingen. Deze codificaties zullen hierna dan ook niet afzonderlijk worden besproken. In plaats daarvan wordt een aantal relevante themata uitgelicht die betrekking hebben op de reikwijdte van deze grondrechten, op de verplichtingen die eruit voortvloeien voor de staat, op hun eventuele horizontale werking en op hun beperkingsmogelijkheden.

De codificaties van het recht op privacy in de Nederlandse Grondwet wijken op een aantal punten af van die in verdragen, in het bijzonder waar het gaat om de beperkingssystematiek. Om die reden wordt hierna wel afzonderlijk aandacht besteed aan art. 10-13 Grondwet.

Het in de inleiding van deze paragraaf benoemde *forum internum* heeft niet in alle grondrechtencodificaties even expliciet bescherming gekregen. Zo reppen art. 6 en 7 Grondwet alleen van de vrijheid een godsdienst te belijden respectievelijk gedachten of gevoelens te openbaren, al is in de totstandkomingsgeschiedenis van deze bepalingen gesteld dat art. 6 Grondwet ook de vrijheid van geweten omvat.[204] Art. 9 EVRM is op dit punt specifieker geformuleerd: het omvat het recht op 'vrijheid van gedachte, geweten en godsdienst', wat eveneens de vrijheid omvat om van godsdienst of overtuiging te veranderen. Art. 10 EVRM vermeldt bovendien expliciet dat de vrijheid van meningsuiting de vrijheid omvat om een mening te koesteren. Belangrijk is dat het hierbij gaat om absolute grondrechten.[205] Waar het uiten van (al dan niet religieuze) meningen en opvattingen beperkt

202 Zie in dit verband met betrekking tot art. 8 EVRM: Verhey 2009, p. 517-535.

203 Zie de toelichtingen op het Handvest bij art. 7 Hv en vgl. art. 52, derde lid Hv.

204 Zie nader Nieuwenhuis 2013b, p. 58. Tijdens de grondwetsherziening van 1983 is tevens uitdrukkelijk gesproken over de mogelijkheid om een afzonderlijk grondrecht op gewetensvrijheid op te nemen, vergelijkbaar met art. 9 EVRM. Uiteindelijk is daartoe niet besloten aangezien de opvatting was dat een houdbare grondwettelijke beperkingsclausule op een dergelijk grondrecht onmogelijk zou zijn; vgl. Vermeulen 1989, p. 142 e.v.

205 Zie reeds EHRM 25 mei 1993, nr. 14307/88, ECLI:CE:ECHR:1993:0525JUD001430788 (*Kokkinakis t. Griekenland*), par. 33. Zie nader Vermeulen & Van Roosmalen 2018, p. 736.

kan worden onder de in het tweede lid vermelde voorwaarden, geldt die mogelijkheid tot beperking niet voor het eigenlijke *hebben* van een bepaalde overtuiging of het *koesteren* van een bepaalde mening.[206] Hetzelfde geldt voor de met art. 9 en 10 EVRM corresponderende bepalingen van het EU-Grondrechtenhandvest, namelijk respectievelijk art. 10 Hv en art. 11 Hv. Art. 10 Hv bevat in zoverre nog wel een verduidelijking van art. 9 EVRM dat het tweede lid bepaalt dat het recht op dienstweigering op grond van gewetensbezwaren wordt erkend. Het gaat dan echter toch weer om het *uiten* van een bepaalde opvatting, en niet om het hebben ervan als zodanig.[207] Soortgelijke bepalingen zijn ten slotte te vinden in art. 18, eerste lid en art. 19, eerste lid IVBPR.

II.1.4 Privacyrechten in de Grondwet

II.1.4.1 Artikel 10 Grondwet

Reikwijdte

Het recht op de eerbiediging van de persoonlijke levenssfeer is in de Nederlandse Grondwet gecodificeerd in art. 10, eerste lid en luidt: 'Ieder heeft behoudens bij of krachtens de wet te stellen beperkingen, recht op de eerbieding van zijn persoonlijke levenssfeer'. Art. 10 is in 1983 in de Nederlandse Grondwet opgenomen. Zoals in de inleiding van deze paragraaf al aangegeven werd daarbij weinig helderheid gegeven over de inhoud en reikwijdte van het begrip 'persoonlijke levenssfeer'. Belangrijk is wel de algemene omschrijving dat het zou gaan om situaties waarin de mens, al dan niet in zelf gekozen gezelschap, onbevangen zichzelf wil zijn. Daarnaast wees de regering op de door art. 12 en art. 13 Gw uitdrukkelijk beschermde woning, briefwisseling en telefoongesprekken, maar ook op het vertrouwelijke gesprek, sommige gewoonten, gedragingen en contacten en bepaalde aspecten van het gezinsleven[208] In de literatuur wordt soms opgemerkt dat het recht op de bescherming van de persoonlijke levenssfeer aangemerkt kan worden als een 'restpost' of 'vangnet' van grondrechten, waaronder dan die onderdelen van het privéleven kunnen worden gevat

206 Idem; zie ook Evans 2001, hst. 5.

207 Tegelijkertijd is van belang dat het onderscheid tussen het hebben en het uiten van een bepaalde overtuiging niet altijd even gemakkelijk is te maken; vgl. Evans 2001, p. 75. Bovendien is het niet altijd nodig of wenselijk om dit te doen. Het HvJ EU overwoog in de zaak *Y en Z* bijvoorbeeld dat het onderscheid niet relevant is als het gaat om de vraag of een vreemdeling bij uitzetting naar het land van herkomst een risico loopt om te worden vervolgd vanwege zijn of haar geloofsovertuiging of religie – in dat geval is enkel relevant dat sprake is van een risico van vervolging, en niet of die vervolging plaatsvindt vanwege het uiten van een geloof of religie, of vanwege het (vermeende) hebben ervan, HvJ EU 5 september 2012, gev. zaken C-71/11 en C-99/11, ECLI:EU:C:2012:518 (*Y. en Z. t. Nederland*), *EHRC* 2003/1 m.nt. B. Aarrass & K.M. de Vries, *JV* 2012/403 m.nt. H. Battjes, par. 62-67.

208 Zie ook Van der Pot 2006, p. 389-390 en Kortmann 2012, p. 477.

die niet uitdrukkelijk door art. 11 tot en met 13 Gw worden gedekt.[209] Dit komt overeen met wat de regering bij de totstandkoming van de Grondwet van 1983 aangaf: het is aan de wetgever en rechter om nader te bepalen welke onderdelen van het privéleven bescherming genieten onder art. 10 Gw.[210]

Bijzondere beperkingsvoorwaarde: formeelwettelijke grondslag

Een beperking op grond van art. 10, eerste lid Gw hoeft niet noodzakelijk te zijn in een democratische samenleving ter bescherming van één of meer specifieke doelen. Wel laat de beperkingsclausule van art. 10, eerste lid Gw alleen beperkingen toe 'bij of krachtens de wet'. Dit komt erop neer dat de beperking gebaseerd moet zijn op een wet in formele zin, waarbij tevens het vereiste geldt dat die formeelwettelijke grondslag voldoende specifiek is. Dat wil zeggen dat een beperking uitdrukkelijk moet zijn vastgelegd in de wet met het oog op een voldoende gespecificeerde situatie.[211] Een generieke mogelijkheid tot beperking van grondrechten de verordenende bevoegdheid van decentrale organen is in strijd met (onder andere) art. 10, eerste lid Gw.

Hoewel voor art. 10, eerste lid Gw geen grote rol is weggelegd in de rechtspraak, zijn er enkele belangrijke uitspraken waarin de beperkingsvoorwaarde van een formeelwettelijke grondslag een rol speelt.[212] Zo valt te wijzen op diverse zaken waarbij volgens de rechter de persoonlijke levenssfeer van de betrokkenen was geschonden doordat bij de opsporing van strafbare feiten gebruik was gemaakt van opsporingsmethoden, terwijl daarvoor destijds onvoldoende wettelijke grondslag bestond.[213] Een ander onderwerp waarbij art. 10, eerste lid Gw werd toegepast is de problematiek inzake het sluiten van een woning die wordt gebruikt voor drugshandel.[214] Daarvoor geldt dat een enkele gemeentelijke verordening niet voldoende is als wettelijke basis; gelet op de aantasting van de privacy die het gevolg is van een geslotenverklaring, is een grondslag in de formele wet vereist. In dezelfde lijn ligt een zaak waarbij een marinier een drankverbod kreeg opgelegd tijdens zijn verblijf op het marineschip, zonder dat daarvoor voldoende wettelijke basis was voorzien,[215] en de uitvoering van onaangekondigde huisbezoeken door interventieteams die waren opgericht om ernstige overlast door jongeren te bestrijden.[216]

209 De Vries 2013. Zie ook Kortmann 2012, p. 477.
210 *Kamerstukken II* 1975/76, 13782, nr. 3, p. 41.
211 ABRvS 28 augustus 1995, *AB* 1996/204 m.nt. L. Rogier (*Drugspand Venlo*).
212 De Vries 2013, p. 152.
213 HR 19 december 1995, *NJ* 1996, 249; HR maart 1996, *NJ* 1997, 86; HR 21 december 2012, *NJ* 2011, 23.
214 ABRvS 28 augustus 1995, *AB* 1996/204 m.nt. L. Rogier (*Drugspand Venlo*).
215 CRvB 3 mei 2002, *AB* 2002/346.
216 Vz Rb Utrecht 25 mei 2007, *NJF* 2007/334.

Positieve verplichtingen
Normaal gesproken hebben de rechten van art. 10-13 Grondwet primair een afweerkarakter: zij beschermen individuen tegen inmenging door de staat in hun privéleven. In een zaak uit 2003 oordeelde de rechtbank Groningen echter dat uit art. 10, eerste lid Gw ook positieve verplichtingen voor de overheid kunnen voortvloeien.[217] In deze zaak oordeelde de rechtbank dat de gemeente en de politieregio Groningen onrechtmatig jegens eisers hadden gehandeld door niet snel genoeg op te treden tegen relschoppers die hun woning belaagden en dat daardoor de persoonlijke levenssfeer van de eisers ernstig was geschaad.

Horizontale werking
Art. 10, eerste lid Gw heeft eveneens betekenis in de relatie tussen burgers (particulieren) onderling. Zoals ook het geval is bij andere grondwetsbepalingen, wordt daarbij echter niet direct de eigenlijke grondwetsbepaling toegepast. In plaats daarvan is er sprake van indirecte horizontale werking van het grondrecht, waarbij het belang van de eerbiediging van de persoonlijke levenssfeer wordt meegewogen bij de invulling van (civiel)wettelijke bepalingen zoals art. 6:162 BW (onrechtmatige daad). Bekend in dit verband is de zaak waarin een bijstandsmoeder werd bespied door haar buurman, die werkzaam was bij de overheidsinstantie die verantwoordelijk was voor het verstrekken van bijstandsuitkeringen.[218] De waarnemingen van de buurman in kwestie hadden als gevolg dat de bijstandsuitkering van de vrouw gedeeltelijk werd ingetrokken. De Hoge Raad oordeelde in deze zaak dat de buurman een onrechtmatige daad had gepleegd jegens de vrouw door inbreuk te maken op haar persoonlijke levenssfeer.

II.1.4.2 Artikelen 11, 12 en 13 Grondwet

De art. 11 (lichamelijke integriteit), 12 (verbod binnentreden zonder toestemming) en 13 Gw (o.a. briefgeheim) bevatten grondrechten die nauw gelieerd zijn aan art. 10 Gw. Het zijn 'gespecificeerde' grondrechten ten opzichte van art. 10 Gw.

Art. 11 Gw reguleert de bescherming van de lichamelijke integriteit.[219] Tijdens de totstandkoming van deze bepaling werd uitdrukkelijk gesteld dat het grondrecht enkel ziet op de bescherming van de fysieke persoon. De geestelijke integriteit – voorzover het niet godsdienstige zaken betrof – diende volgens de toenmalige regering niet onder de reikwijdte van art. 11 Gw, maar onder die van art. 10 Gw te vallen.[220] Dit gegeven laat zien dat art.

217 Rb Groningen 22 januari 2003, *NJ* 2003, 169.
218 HR 9 januari 1987, *NJ* 1987/928 (*Edamse bijstandsmoeder*). Zie over het leerstuk van horizontale werking van grondrechten in de Grondwet onder meer Verhey 1992 en Nehmelman & Noorlander 2013.
219 Zie nader over deze bepaling ook Van Sasse van Ysselt 2017, p. 403 e.v.
220 *Kamerstukken II* 1979/80, 16 086, nr. 8, p. 3.

10 Gw geldt als 'restbepaling' ten opzichte van de meer gespecificeerde bepalingen zoals neergelegd in de art. 11-13 Gw.

De reikwijdte van art. 11 Gw ziet, gelet op de toelichting van de regering destijds, op vele situaties. De regering noemde achtereenvolgens: foltering, lijfstraffen, lichamelijke en geestelijke mishandeling, gedwongen medische experimenten, toedienen van elektroshocks aan psychisch gestoorden, gedwongen behandeling van geslachtsziekten, gedwongen toediening van voedsel aan hongerstakers, toediening van waarheidsserum aan verdachten, leegpompen van de maag, encefalografie, bloedafname, inenting, röntgenologisch onderzoek, verwondingen, operaties, behandeling door een arts, het ondergaan van medische keuringen en het knippen van de haren.[221] De bepaling beperkt zich tot *lichamelijke* integriteit, dus de onaantastbaarheid van het menselijk lichaam.[222] Weliswaar achtte de regering ook de geestelijke integriteit beschermwaardig, maar belangrijke bescherming werd volgens de regering op dat punt al geboden door de bepalingen over de vrijheid van godsdienst en levensovertuiging, de vrijheid van meningsuiting en de vrijheid van onderwijs.[223] In zekere zin is dit opmerkelijk, nu hiervoor al is opgemerkt dat de grondwettelijke bepalingen over godsdienstvrijheid en vrijheid van meningsuiting het *forum internum* niet expliciet beschermen. Aangenomen moet dan ook worden dat deze rechten impliciet en inherent in de tekst ervan besloten liggen. Daarnaast kan worden aanvaard dat niet expliciet afgedekte aspecten van het recht op geestelijke integriteit beschermd worden door de restbepaling van art. 10 Gw.[224]

Er bestaat nogal wat discussie over de vraag of art. 11 Gw alleen een afweerrecht omvat of ook een positief beschikkingsrecht. Het lijstje van voorbeelden van gevallen waarop de bepaling van toepassing is, lijkt op het eerste te wijzen: de overheid mag niet actief ingrijpen in iemands lichamelijke integriteit. Tegelijkertijd is er in de literatuur ook wel op gewezen dat ook het recht op de vrije beschikking over het eigen lichaam, door het artikel kan worden afgedekt.[225] Noch in de literatuur, noch in de rechtspraak is echter een eensluidend antwoord te vinden op de vraag of een recht op beschikking over het eigen lichaam wordt beschermd door art. 11 Gw.[226]

Net als art. 10 Gw laat art. 11 Gw beperkingen toe 'bij of krachtens de wet'.[227] Daarbij geldt dus dat voldoende specifieke delegatie door de formele wetgever is toegestaan, vergelijkbaar met hetgeen hiervoor is gezegd over de beperkingssystematiek van art. 10 Gw. Gelet hierop maakt de vraag of geestelijke integriteit en zelfbeschikking onder of art. 10

221 *Kamerstukken II* 1978/79, 15 463, nr. 2, p. 4.
222 Gerards, Koffeman & Hendriks 2013, p. 79.
223 Gerards, Koffeman & Hendriks 2013, p. 79; zie nader MvT bij art. 11 Grondwet, *Kamerstukken II* 1979/80, 16 086, nr. 3, p. 4.
224 Gerards, Koffeman & Hendriks 2013, p. 79. Vgl. ook Van Sasse van Ysselt 2017, p. 404 e.v.
225 Van Beers 2009, p. 114 e.v.
226 Gerards, Koffeman & Hendriks 2013, p. 82.
227 Zie nader ook Van Sasse van Ysselt 2017, p. 406.

Gw of onder art. 11 Gw valt alleen uit voor de vraag onder welke wetsbepaling de reikwijdte valt; voor wat betreft de mogelijkheden tot beperking is er weinig verschil. De ruime beperkingsbevoegdheid heeft, samen met de ruime reikwijdte van art. 11 Gw, overigens wel tot gevolg dat er nogal wat wetgeving bestaat die (een inbreuk op) de lichamelijke integriteit reguleert, zoals de regeling inzake adem- en bloedonderzoek bij bepaalde verkeersovertredingen.[228] Om die reden is het niet verrassend dat de inhoudelijk veel meer sturende rechtspraak van het EHRM in de praktijk meer betekenis heeft dan art. 11 Gw voor het reguleren van het recht op lichamelijke integriteit.[229]

Art. 12 Gw bepaalt uitdrukkelijk dat binnentreden in een woning 'tegen de wil' van de bewoner niet is toegestaan. Ook een woonwagen, een studentenhuis of woongroep vallen onder de bescherming van dit grondrecht.[230] Zowel huiseigenaren als huurders vallen onder de definitie van 'bewoner'. Art. 12 Gw geeft, gelet op de memorie van toelichting bij deze bepaling, vermoedelijk geen bescherming voor het eigendom of de huur van de woning; de reikwijdte betreft alleen de bescherming van het ongestoorde gebruik van de woning.[231] De mogelijkheden tot beperking van dit grondrecht zijn op dezelfde manier gereguleerd als het geval is voor art. 10 en 11 Gw. Belangrijke beperkingsmogelijkheden voor dit grondrecht zijn onder meer neergelegd in de Algemene wet op het binnentreden. Art. 138 Sr regelt bovendien de strafbaarstelling van het wederrechtelijk binnendringen in een woning (door derden).

Art. 13 Gw voorziet ten slotte in de bescherming van het brief-, telefoon- en telegraafgeheim. Bij de wet geregelde gevallen zijn op last van de rechter of met machtiging van hen die daartoe bij de wet zijn aangewezen (lid 2). Als voorbeeld kan in dit verband worden gewezen op de opsporingsbevoegdheden uit het Wetboek van Strafvordering die het opnemen en onderzoek van vertrouwelijke communicatie reguleren.[232] De opkomst van tal van nieuwe communicatiemiddelen heeft de vraag doen rijzen of art. 13 Gw gewijzigd zou moeten worden en of nieuwe vormen van communicatie eveneens onder de bescherming van art. 13 Gw zouden moeten vallen. Een voorstel van die strekking is gedaan in 2000 door de Commissie Grondrechten in het digitale tijdperk. Deze commissie stelde een techniekonafhankelijke formulering voor van onder andere art. 13 Gw. In 2010 werd dit voorstel nog eens herhaald door de Staatscommissie Grondwet. Inmiddels heeft de wetgever

228 Zie voor een overzicht: Van Sasse van Ysselt 2017, p. 412 e.v.; Loof 2013.
229 Gerards, Koffeman & Hendriks 2013, p. 85.
230 *Kamerstukken II* 1984/85, 19 073, nr. 3, p. 20.
231 *Kamerstukken II* 1984/85, 19 073, nr. 3, p. 20.
232 Art. 126l t/m 126nb, 126s t/m 126ub en 126zf t/m 126zja Sv.

gehoor gegeven aan deze oproep en zal art. 13 Gw een nieuwe formulering krijgen die meer in overeenstemming is met de technologische ontwikkelingen.[233]

Net als de andere bepalingen uit de Grondwet, heeft ook art. 13 Gw geen directe horizontale werking. De wetgever heeft daarvoor wel enkele specifieke wettelijke voorzieningen gecreëerd, bijvoorbeeld in de Postwet 2009 en in de Telecommunicatiewet 186.[234]

II.1.5 Privacyrechten in Europese en internationale verdragen

II.1.5.1 Inleiding

Hierboven is al aangegeven dat privacyrechten en daaraan verwante rechten (zoals het *forum internum*, de menselijke waardigheid, persoonlijke autonomie en het persoonlijkheidsrecht) zijn gecodificeerd in verschillende Europese en internationale verdragen. Voor dit onderzoek het meest van belang zijn het EVRM en het Handvest. Het EHRM en het HvJ EU hebben inmiddels een ruime rechtspraak tot stand gebracht over de relevante bepalingen. In het navolgende worden daarvan de hoofdpunten besproken.

II.1.5.2 Reikwijdte

Begripsbepaling, typologieën en indelingen

Al van oudsher wordt aangenomen dat geen duidelijk onderscheid kan worden gemaakt tussen het recht op respect voor het privéleven en de andere in art. 8 EVRM genoemde rechten.[235] In dit verband kan worden gewezen op een resolutie van de Raadgevende Vergadering van de Raad van Europa uit 1970 waarin het recht op privacy als volgt wordt omschreven:

> 'The right to privacy consists essentially in the right to live one's own life with a minumum of interference. It concerns private, family and home life, physical and moral integrity, honour and reputation, avoidance of being placed in a false light, non-revelation of irrelevant and embarrassing facts, unauthorised publication of private photographs, protection from disclosure of information given or received by the individual confidentially.'[236]

---

233 De eerste lezing van dit grondwetswijzigingsvoorstel is inmiddels in het Staatsblad geplaatst: *Stb.* 2017, 334. Het artikel komt, indien het de tweede lezing (*Kamerstuknr.* 33989) doorkomt, als volgt te luiden: '1. Ieder heeft recht op eerbiediging van zijn brief- en telecommunicatiegeheim. 2. Beperking van dit recht is mogelijk in de gevallen bij de wet bepaald met machtiging van de rechter of, in het belang van de nationale veiligheid, door of met machtiging van hen die daartoe bij de wet zijn aangewezen.'

234 Kortmann 2012, p. 487.

235 Zie reeds Van Dijk & Van Hoof 1998, p. 489, verwijzend naar ECieRM 10 juli 1978, nr. 8257, *DR* 13, p. 248 (*X t. Zwitserland*).

236 Resolutie 428, (1970), Council of Europe 1979, p. 908.

Ten aanzien van het begrip privéleven ('private life') zoals neergelegd in art. 8 EVRM heeft Wiarda bovendien opgemerkt dat het behoort tot de allervaagste begrippen die de Conventie kent. Zo stelde hij in 1987:

> 'Er is vrijwel niets in het leven van een mens dat niet op een of andere wijze een als "private" te beschouwen aspect daarvan raakt, en er is nauwelijks enige "interference by public authority" met het doen en laten van mensen denkbaar dat op het "private life" geen invloed heeft of kan hebben.'[237]

Het EHRM heeft vanwege de onbepaaldheid van het begrip ook nooit een uitputtende, eenduidige definitie van het begrip willen geven.[238] In plaats daarvan hebben het EHRM, en overigens ook het HvJ EU, het begrip privéleven in de afgelopen decennia vooral ingekleurd en uitgelegd door toepassing in concrete feitencomplexen. De toepassing van dit begrip komt daarbij goed overeen met de hierboven weergegeven definitie van de Raadgevende Vergadering van de Raad van Europa uit 1970. Er zijn diverse verschillende indelingen te geven van deze rechtspraak. Zo hebben Koops e.a. onderscheid gemaakt tussen verschillende vormen van privacy, geplaatst op assen die lopen van privacy op meer persoonlijk vlak (bijvoorbeeld lichamelijke integriteit) tot meer publiek terrein (bijvoorbeeld privacy ten aanzien van het eigen gedrag), en een as waarbij het accent meer ligt op individuele vrijheid (het recht om vrij te blijven van overheidsbemoeienis, 'being let alone') of meer op zelfontplooiing.[239] Daardoor onderscheiden zij maar liefst acht verschillende vormen van privacy: lichamelijk, geestelijk, ruimtelijk, ten aanzien van besluitvorming, ten aanzien van communicatie, relationeel, ten aanzien van eigendom en ten aanzien van gedrag. Ten aanzien van alle acht vormen zien zij bovendien nog een negende, overlappende vorm van privacy, namelijk informationele privacy. Ook anderen, zoals Solove, hebben gepoogd om een taxonomie van privacy te maken, waarbij verschillende vormen en verschillende rationales worden onderscheiden.[240]

De waarde van deze theoretische typologieën en taxonomieën is groot, zeker waar het gaat om het verkrijgen van een goed begrip van het privacybegrip. Niettemin wordt in het navolgende gekozen voor een indeling aan de hand van de karakterisering die de Europese hoven zelf geven, eerder dan een indeling aan de hand van deze theoretische typologieën. Het voordeel daarvan is dat in ieder geval duidelijk is dat de hierna besproken deelvormen

237 Wiarda 1987.

238 Zie reeds EHRM 16 december 1992, nr. 13710/88, ECLI:CE:ECHR:1992:1216JUD001371088 (*Niemietz t. Duitsland*), *NJ* 1993/400, m.nt. E.J. Dommering, par. 29; dit is inmiddels onderdeel van zijn vaste rechtspraak en wordt in vrijwel iedere uitspraak herhaald, zoals recent nog in EHRM 9 januari 2018, nrs. 1874/13 en 8567/13, ECLI:CE:ECHR:2018:0109JUD000187413 (*López Ribalda e.a. t. Spanje*), *JAR* 2018/56 m.nt. I.J. de Laat, par. 54.

239 Koops e.a. 2017, p. 564 e.v.

240 Solove 2006; zie voor nadere voorbeelden van typologieën ook Koops e.a. 2017, p. 494 e.v.

expliciet worden beschermd door de bindende Europese grondrechteninstrumenten. Wel wordt hier en daar, ter verheldering, de rechtspraak gerelateerd aan de typologie van Koops e.a.

Zoals eerder al toegelicht blijft het recht op bescherming van persoonsgegevens en daaraan direct gerelateerde rechten hierna buiten beschouwing. Dit betekent ook dat de rechtspraak van het HvJ EU over art. 7 Hv hierna maar beperkt aan de orde komt, nu veruit de meeste uitspraken van het HvJ over privacy betrekking hebben op persoonsgegevens.[241] Het accent ligt daarmee op de rechtspraak van het EHRM.

In de Europese rechtspraak erkende privacyrechten

1. Allereerst behoort het klassieke begrip 'privacy' tot de rechten die door EVRM en EU-Grondrechtenhandvest worden beschermd. Het gaat dan om een set van rechten die verband houden met de privéomgeving – het recht om vrij te zijn in de eigen woning of de eigen auto, om vrij te communiceren (via telefoon, sociale media of andere middelen), om zich vrij te kunnen bewegen en om zijn eigendommen naar eigen inzicht te kunnen gebruiken.[242] In de rechtspraak komen deze privacyrechten vooral tot uitdrukking in de volgende situatietypes:
2. *Afluisteren en onderscheppen van communicatie*: het gebruik van geheime opsporingsmethoden, zoals het afluisteren van telefoons, het plaatsen van GPS-detectiemiddelen in iemands auto, of het onderscheppen van iemands post, vormt volgens vaste rechtspraak een inbreuk op het recht op respect voor het privéleven en de correspondentie.[243] Veelal kunnen degenen die getroffen worden door geheime opsporingsmethoden dit niet bewijzen, eenvoudigweg doordat zij niet op de hoogte zijn van het onderscheppen van hun communicatie. Het EHRM ondervangt dit door te aanvaarden dat ook de *mogelijkheid* van het onderscheppen of afluisteren van post of telefoongesprekken moet worden gezien als een beperking van de vrijheid van het individu om van deze communicatiemiddelen gebruik te maken.[244]

---

241 Greer, Gerards & Slowe 2018, p. 334.

242 Zie ook Koops e.a. 2017, par. 4.3, die deze vormen samenvatten onder het cluster 'Privacy of Places or Property'.

243 Zie klassiek bijv. EHRM 6 september 1978, nr. 5029/71, ECLI:CE:ECHR:1978:0906JUD000502971 (*Klass e.a. t. Duitsland*), *NJ* 1979/327 m.nt. E.A. Alkema, par. 41; EHRM 2 augustus 1984, nr. 8691/79, ECLI:CE:ECHR:1984:0802JUD000869179 (*Malone t. het Verenigd Koninkrijk*), *NJ* 1988/534 m.nt. P. van Dijk, par. 64. Zie ten aanzien van het afluisteren van gesprekken recenter het gezaghebbende arrest EHRM (GK) 4 december 2015, nr. 47143/06, ECLI:CE:ECHR:2015:1204JUD004714306 (*Roman Zakharov t. Rusland*), *EHRC* 2016/87 m.nt. M. Hagens, *NJ* 2017/185 m.nt. E.J. Dommering; zie over GPS-toezicht bijv. EHRM 2 september 2010, nr. 35623/05, ECLI:CE:ECHR:2010:0902JUD003562305 (*Üzun t. Duitsland*), *EHRC* 2010/123 m.nt. P. de Hert & J. van Caeneghem; zie ten aanzien van het openen van post bijv. EHRM 31 oktober 2017, nr. 22767/08, ECLI:CE:ECHR:2017:1031JUD002276708 (*Dragoş Ioan Rusu t. Roemenië*), *EHRC* 2018/13 m.nt. D.A.G. van Toor.

244 EHRM 6 september 1978, nr. 5029/71, ECLI:CE:ECHR:1978:0906JUD000502971 (*Klass e.a. t. Duitsland*), *NJ* 1979/327 m.nt. E.A. Alkema, par. 34-36 en 41.

3. *Doorzoeking van eigendommen*: tot de intieme sfeer van het privéleven behoren ook de eigen woning en zaken als tassen, koffers of laptops ('proprietary privacy'). Het doorzoeken van deze eigendommen (bijvoorbeeld bij een huiszoeking of bij fouilleren) vormt dan ook een inbreuk op het recht op respect voor het privéleven. Het EHRM en het HvJ EU hebben daarbij het bereik van dit recht ruim geformuleerd: hieronder vallen niet alleen de directe privéomgeving, maar ook meer professionele of werkgerelateerde omgevingen, zoals kantoorgebouwen, werkcomputers of laptops.[245] Overigens erkent het HvJ wel een iets minder ruime reikwijdte voor dit recht dan het EHRM.[246]
4. *Gebruik van bewakingscamera's of van verborgen camera's*: ook het maken van opnames met bewakingscamera's of verborgen camera's kan een inbreuk vormen op de privacy wanneer mensen niet kunnen verwachten dat ze worden gefilmd. Als bewakingscamera's op de openbare weg hangen, is dat anders; in dat geval kan voor mensen bekend zijn dat ze in de gaten worden gehouden.[247] Er is volgens het EHRM dan geen sprake van een inbreuk op het recht op privéleven.[248] Datzelfde geldt als opnamen met een verborgen camera worden gemaakt in een verder openbare ruimte, omdat ook dan mensen niet kunnen verwachten dat ze niet door andere worden gezien.[249] Als mensen niet kunnen vermoeden dat ze worden gefilmd, bijvoorbeeld omdat ze in een privéomgeving zijn, kan er wel een redelijke verwachting van privacy bestaan.[250]
5. In de tweede plaats is er in de rechtspraak van het EHRM en het HvJ een aantal rechten erkend dat samenhangt met de *persoonlijke identiteit*.[251] Deze rechten zijn sterk ingekleurd aan de hand van de hierboven besproken noties van menselijke waardigheid en persoonlijk autonomie. Tot deze categorie behoren (niet-limitatief) de volgende elementen:
6. *Naam*: een naam is behalve de uitdrukking van een verbintenis met familieleden, ook een middel tot identificatie, zowel voor de betrokkene zelf (zelfidentificatie) als voor

245 Zie voor het eerste klassiek reeds EHRM 16 december 1992, nr. 13710/88, ECLI:CE:ECHR:1992:1216JUD001371088 (*Niemietz t. Duitsland*), *NJ* 1993/400, m.nt. E.J. Dommering resp. HvJ EG 22 oktober 2002, zaak C-94/00, ECLI:EU:C:2002:603 (*Roquette Frères SA*), *NJ* 2003/453, m.nt. M.R. Mok; zie voor het laatste bijv. EHRM 13 februari 2018, nr. 61064/10, ECLI:CE:ECHR:2018:0213JUD006106410 (*Ivashchenko t. Rusland*); EHRM 22 februari 2018, nr. 588/13, ECLI:CE:ECHR:2018:0222JUD000058813 (*Libert t. Frankrijk*).

246 Vgl. bijv. HvJ EU 18 juni 2015, zaak C-583/13 P, ECLI:EU:C:2015:404 (*Deutsche Bahn*), par. 20.

247 EHRM 28 januari 2003, nr. 44647/98, ECLI:CE:ECHR:2003:0128JUD004464798 (*Peck t. het Verenigd Koninkrijk*), *EHRC* 2003/24, par. 59; EHRM 17 juli 2003, nr. 63737/00 (*Perry t. Verenigd Koninkrijk*), *NJ* 2006/40 m.nt. E.J. Dommering, *EHRC* 2003/79, par. 40-43.

248 Idem.

249 Zie bijv. EHRM 22 februari 2018, nr. 72562/10, ECLI:CE:ECHR:2018:0222JUD007256210 (*Alpha Doryforiki Tileorasi Anonymi Etairia t. Griekenland*).

250 Zie bijv. EHRM 28 november 2017, nr. 70838/13, ECLI:CE:ECHR:2017:1128JUD007083813 (*Antović en Mirković t. Montenegro*), *JAR* 2018/20.

251 Zie nader bijv. Koffeman 2015, C.3.

anderen.[252] De beide Europese hoven hebben dan ook aangenomen dat beperkingen op het kunnen voeren van een naam of, bijvoorbeeld, de schrijfwijze ervan, een inbreuk vormen op het privéleven.[253]

7. *Kennen van afstamming en familierelaties*: onder het recht op privéleven valt tevens het kennen van de identiteit van de ouders en andere familieleden en de omstandigheden waarin het individu is opgegroeid.[254]
8. *Genderidentiteit*: iemands genderidentiteit is volgens het EHRM een fundamenteel onderdeel van het privéleven. Daaruit vloeit het recht voort dat een persoon zelf aan kan geven of hij/zij zich als man of vrouw wil identificeren.[255] Dit behoort volgens het Straatsburgse Hof tot de meest basale aspecten van de mogelijkheid tot zelfbeschikking. Ook de juridische erkenning van een geslachtsveranderende operatie valt binnen het bereik van het privéleven, net als de toegang tot een dergelijke operatie.[256]
9. *Uiterlijk*: keuzes voor bepaalde kleding vallen eveneens binnen het bereik van art. 8 EVRM, zoals de keuze om hoofdbedekking of een baard te dragen om andere dan religieuze redenen. Zijn er wel religieuze motieven, dan valt de kledingkeuze binnen het bereik van het *forum externum* van art. 9 EVRM.[257]
10. *Seksuele gerichtheid en seksuele activiteit*: volgens het EHRM is het hebben van een bepaalde seksuele oriëntatie en de mogelijkheid om daarnaar te leven een intiem aspect van het recht op privéleven.[258] Ook iemands seksleven valt binnen het bereik van het

252 Zie bijv. EHRM 11 september 2007, nr. 59894/00, ECLI:CE:ECHR:2007:0911JUD005989400 (*Bulgakov t. Oekraïne*), par. 51. Vgl. ook De Vries 2013, p. 135.

253 Idem en zie bijv. HvJ EG 2 oktober 2003, zaak C-148/02, ECLI:EU:C:2003:539 (*Garcia Avello*), par. 42; HvJ EU 22 december 2010, zaak C-208/09 (*Sayn-Wittgenstein*), ECLI:EU:C:2010:806, *NJ* 2011/119 m.nt. M.R. Mok, par. 52; HvJ EU 12 mei 2011, zaak C-391/09, ECLI:EU:C:2011:291 (*Runevič-Vardyn en Wardyn*), *NJ* 2011/421, m.nt. M.R. Mok; HvJ EU 2 juni 2016, zaak C-438/14, ECLI:EU:C:2016:401 (*Bogendorff von Wolffersdorff*), *EHRC* 2016/202 m.nt. D.A.J.G. de Groot.

254 Zie klassiek bijv. EHRM 7 juli 1989, nr. 10454/83, ECLI:CE:ECHR:1989:0707JUD001045483 (*Gaskin t. het Verenigd Koninkrijk*), *NJ* 1991/659 m.nt. E.J. Dommering, par. 49; EHRM 7 februari 2002, nr. 53176/99, ECLI:CE:ECHR:2002:0207JUD005317699 (*Mikulić t. Kroatie*), *EHRC* 2002/25 m.nt. H.L. Janssen, par. 54; EHRM (GK) 13 februari 2003, nr. 42326/98, ECLI:CE:ECHR:2003:0213JUD004232698 (*Odièvre t. Frankrijk*), *EHRC* 2003/29, *NJ* 2003/587 m.nt. S. Wortmann, par. 29. Zie nader Koffeman 2015, C.3.3.1.

255 Zie klassiek EHRM (GK) 11 juli 2002, nr. 28957/95, ECLI:CE:ECHR:2002:0711JUD002895795 (*Christine Goodwin t. het Verenigd Koninkrijk*), *EHRC* 2002/74 m.nt. H.L. Janssen & J. van der Velde, par. 77; EHRM 12 juni 2003, nr. 35968/97, ECLI:CE:ECHR:2003:0612JUD003596897 (*Van Kück t. Duitsland*), *EHRC* 2003/61 m.nt. J.H. Gerards, AB 2003/437 m.nt. B. van Beers, par. 73 en 75.

256 EHRM (GK) 11 juli 2002, nr. 28957/95, ECLI:CE:ECHR:2002:0711JUD002895795 (*Christine Goodwin t. het Verenigd Koninkrijk*), *EHRC* 2002/74 m.nt. H.L. Janssen & J. van der Velde resp. EHRM 10 maart 2015, nr. 14793/08, ECLI:CE:ECHR:2015:0310JUD001479308 (*Y.Y. t. Turkije*), *EHRC* 2015/106 m.nt. J.H. Gerards.

257 Zie over een en ander EHRM (GK) 1 juli 2014, nr. 43835/11, ECLI:CE:ECHR:2014:0701JUD004383511 (*S.A.S. t. Frankrijk*), *EHRC* 2014/208 m.nt. P.B.D.D.F. van Sasse van Ysselt, par. 106.

258 Zie reeds EHRM 22 oktober 1981, nr. 7525/76, ECLI:CE:ECHR:1981:1022JUD000752576 (*Dudgeon t. het Verenigd Koninkrijk*), par. 52; EHRM (GK) 27 september 1999, nrs. 33985/96 en 33986/96, ECLI:CE:ECHR:1999:0927JUD003398596 (*Smith en Grady t. het Verenigd Koninkrijk*), par. 89-90.

privéleven, ook als het gaat om seksuele activiteiten die eventueel schadelijk zijn voor de betrokkene.[259]

11. Het EHRM erkent daarnaast het belang van de ontwikkeling van iemands *sociale identiteit* en het recht om relaties aan te gaan met anderen en met de omgeving ('the outside world').[260] Het gaat hierbij in belangrijke mate om relationele privacy.[261] Hiertoe behoren onder meer de volgende aspecten:
12. Het *aangaan van relaties met anderen*, zoals partnerschappen tussen mensen van gelijk geslacht, heeft het EHRM een tijdlang alleen gezien als onderdeel van het privéleven.[262] Inmiddels heeft het echter erkend dat hieraan de meer specifieke bescherming toekomt van het recht op respect voor het gezinsleven.[263]
13. *Toegang tot beroepen en zakelijke relaties*: niet alleen de huiselijke of familiaire sfeer vallen onder de bescherming van het recht op privéleven zoals neergelegd in art. 8 EVRM, maar ook de werkomgeving.[264] Als iemand bijvoorbeeld een beroepsverbod krijgt opgelegd of wordt ontslagen, dan raakt dit hem of haar in de privésfeer.[265]
14. *Banden met het land van verblijf*: personen die niet de nationaliteit van een verdragsstaat hebben, genieten in beginsel geen recht op grond van art. 8 EVRM om in een (verdrags)staat te verblijven.[266] Als vreemdelingen eenmaal in een bepaald land verblijven, erkent het EHRM echter dat de persoonlijke, sociale en economische banden die zij in het gastland opbouwen, deel uitmaken van hun privéleven.[267] Gedacht kan in dit verband worden aan relaties die ontstaan doordat een vreemdeling in het gastland onderwijs volgt, er arbeid verricht of op andere wijze is geïntegreerd in de samenleving. Dit kan betekenen dat uitzetting van geïntegreerde vreemdelingen een inmenging kan zijn in

259 EHRM 17 februari 2005, nrs. 42758/98 en 45558/99, ECLI:CE:ECHR:2005:0217JUD004275898 (*K.A. en A.D. t. België*), *EHRC* 2005/38, par. 83. Zie verder Koffeman 2015, C.3.5. en De Vries 2018, p. 685.

260 Bijv. EHRM 16 december 1992, nr. 13710/88, ECLI:CE:ECHR:1992:1216JUD001371088 (*Niemietz t. Duitsland*), *NJ* 1993/400 m.nt. E.J. Dommering, par. 29; EHRM (GK) 4 december 2008, nrs. 30562/04 en 30566/04, ECLI:CE:ECHR:2008:1204JUD003056204 (*S. en Marper t. het Verenigd Koninkrijk*), *EHRC* 2009/13 m.nt. B.J. Koops, *NJ* 2009/410 m.nt. E.A. Alkema, par. 66.

261 Vgl. ook Koops e.a. 2017, p. 521 e.v.

262 Zie EHRM 24 juni 2010, nr. 30141/04, ECLI:CE:ECHR:2010:0624JUD003014104 (*Schalk en Kopf t. Oostenrijk*), *EHRC* 2010 m.nt. N.R. Koffeman, par. 90-95.

263 Idem, par. 95. Koops e.a. 2017, p. 521 e.v. rekenen ook familie- en gezinsrelaties tot de privacy; dat is in ruimere zin correct, maar omdat gezinsleven voor het EVRM en het Hv een aparte categorie is, wordt deze hier niet verder behandeld. Zie over gezinsleven wel ook uitgebreid De Vries 2018; Forder 2015.

264 EHRM 16 december 1992, nr. 13710/88, ECLI:CE:ECHR:1992:1216JUD001371088 (*Niemietz t. Duitsland*), *NJ* 1993/400, m.nt. E.J. Dommering, par. 29.

265 Zie bijv. EHRM (GK) 12 juni 2014, nr. 56030/07, ECLI:CE:ECHR:2014:0612JUD005603007 (*Fernández Martínez t. Spanje*), *EHRC* 2014/219 m.nt. A. Overbeeke; EHRM 27 juli 2004, nr. 55480/00, ECLI:CE:ECHR:2004:0727JUD005548000 (*Sidabras en Džiautas t. Litouwen*), *EHRC* 2004/90, m.nt. Gerards. Zie nader De Vries 2018, p. 687; Koffeman 2015, C.3.9.

266 De Vries 2018, p. 689.

267 EHRM (GK) 9 oktober 2003, nr. 48321/99, ECLI:CE:ECHR:2003:1009JUD004832199 (*Slivenko t. Letland*), *EHRC* 2003/91 m.nt. H.L. Janssen, par. 69; zie nader De Vries 2018, p. 689 e.v.

hun recht op privéleven.[268] Ook in het EU-recht worden de opgebouwde banden met het gastland erkend en moeten deze worden gerespecteerd bij bijvoorbeeld beslissingen tot uitzetting.[269]

15. In de Europese rechtspraak is ook het recht op *lichamelijke en geestelijke integriteit* erkend als onderdeel van het privéleven.[270] In het EU-recht is het recht op 'menselijke integriteit' bovendien afzonderlijk beschermd in art. 3 Hv, maar vooralsnog heeft het geen eigen rol gespeeld in de rechtspraak van het HvJ.[271] Daarbij geldt wel dat bepaalde aspecten van deze integriteit niet zozeer worden beschermd door art. 8 EVRM resp. art. 7 Hv, maar door het verbod van onmenselijke en vernederende behandeling van art. 3 EVRM resp. art. 4 Hv. Het gaat dan vooral om zeer vergaande inbreuken, zoals dwangbehandeling, gedwongen sterilisatie of gedwongen voeding bij hongerstakingen.[272] In de iets minder ernstige gevallen wordt meestal de algemene privacybepaling toegepast. Het EHRM heeft daarbij erkend dat deze integriteit een cruciaal onderdeel van het privéleven vormt.[273] Ook dan is dit aspect van het recht op respect voor het privéleven echter alleen aan de orde als sprake is van een nadelig effect van enige ernst ('minimum level of severity').[274] Binnen dit deelrecht zijn in de rechtspraak weer verschillende afzonderlijke rechten te onderscheiden, die allemaal nauw samenhangen met de hiervoor al benoemde waarden van persoonlijke autonomie en menselijke waardigheid:
16. Het moeten dragen van handboeien of lijfsvisitatie kunnen onder omstandigheden onder het recht op respect voor het privéleven vallen, in het bijzonder wanneer de drempel om te kunnen spreken van een vernederende en onmenselijke behandeling (art. 3 EVRM, art. 4 Hv) niet is overschreden.[275]
17. Geïnformeerde toestemming is in beginsel vereist wanneer sprake is van *medisch onderzoek en medische behandeling*.[276] Ook wanneer het weigeren van een behandeling

---

268 Idem.

269 Zie bijv. HvJ EU 13 september 2016, zaak C-165/14, ECLI:EU:C:2016:675 (*Rendón Marín*), *JV* 2016/201, par. 66.

270 Zie reeds EHRM 26 maart 1985, nr. 8978/80, ECLI:CE:ECHR:1985:0326JUD000897880 (*X. en Y. t. Nederland*), *NJ* 1985/525 m.nt. E.A. Alkema, *NJCM-Bull.* 1985, p. 410 m.nt. J.G.C. Schokkenbroek, par. 22. Zie verder uitgebreid Gerards, Koffeman & Hendriks 2013 en zie Van Sasse van Ysselt 2017, p. 408.

271 Greer, Gerards & Slowe 2018, p. 330.

272 Zie nader, met verdere bronvermeldingen, Gerards 2015, p. 310 e.v. en zie Koffeman 2015, C.3.6.

273 Zie bijv. EHRM 6 februari 2001, nr. 44599/98, ECLI:CE:ECHR:2001:0206JUD004459998 (*Bensaid t. het Verenigd Koninkrijk*), *NJ* 2001/549, *JV* 2001/103 m.nt. Wouters.

274 Zie bijv. EHRM 8 juli 2003 (ontv.), nr. 27677/02, ECLI:CE:ECHR:2003:0708DEC002767702 (*Sentges t. Nederland*), *EHRC* 2003/75 m.nt. E. Brems, *NJCM-Bull.* 2004, m.nt. A.C. Hendriks, p. 54.

275 Zie bijv. EHRM 26 september 2006, nr. 12350/04, ECLI:CE:ECHR:2006:0926JUD001235004 (*Wainwright t. het Verenigd Koninkrijk*), *EHRC* 2006/130 m.nt. G. De Jonge; zie nader Koffeman 2015, C.3.6.3.

276 EHRM 22 juli 2003, nr. 24209/94, ECLI:CE:ECHR:2014:1106JUD001292713 (*Y.F. t. Turkije*), *EHRC* 2003/80 m.nt. K. Henrard, par. 33; EHRM 16 juni 2005, nr. 61603/00, ECLI:CE:ECHR:2005:0616JUD006160300 (*Storck t. Duitsland*), *EHRC* 2005/82 m.nt. J. van der Velde, par. 143; EHRM 7 oktober 2008, nr. 35228/03, ECLI:CE:ECHR:2008:1007JUD003522803 (*Bogumil t. Portugal*), *NJ* 2010/58 m.nt. F.C.B. van Wijmen, par. 84; EHRM 2 juni 2009, nr. 31675/04, ECLI:CE:ECHR:2009:0602JUD003167504 (*Codarcea t. Roemenië*),

ernstige of zelfs fatale gevolgen zou hebben, moet de keuze van de betrokkene worden gerespecteerd.[277]

18. Wanneer iemands toegang tot financiële middelen zodanig wordt beperkt dat bijvoorbeeld de *toegang tot de gezondheidszorg* onder druk komt te staan, bijvoorbeeld door het bevriezen van iemands tegoeden, kan dit volgens het HvJ ook inbreuk maken op het privéleven.[278]
19. Het ontnemen van *handelingsbekwaamheid* maakt volgens het EHRM eveneens inbreuk op het privéleven,[279] net als het onder curatele plaatsen van iemand die beweerdelijk niet goed in staat is zijn eigen belangen te behartigen.[280]
20. Het EHRM heeft erkend dat bij *vrijwillige levensbeëindiging* en bij het *beëindigen van een levensreddende behandeling* sprake is van situaties die samenhangen met de persoonlijke autonomie behorend bij het recht op privéleven.[281]
21. Ten slotte heeft het EHRM met behulp van de noties van persoonlijke autonomie en het recht op fysieke en mentale integriteit de toegang tot *abortus* binnen het bereik van art. 8 EVRM gebracht.[282]
22. Onder het recht op privéleven vallen ook *reproductieve rechten*, waaronder het recht om (genetisch aan de ouder verwante) kinderen te krijgen.[283] Ook het recht op kunstmatige voortplanting en de toegang tot de daarvoor benodigde technieken, waaronder

---

EHRC 2009/96 m.nt. E.H. Hulst; EHRM 6 november 2014, nr. 12927/13, ECLI:CE:ECHR:2014:1106JUD001292713 (*Dvořáček t. Tsjechië*), *EHRC* 2015/21 m.nt. A.C. Hendriks. Zie verder, met meer detail en nadere bronvermeldingen, Gerards 2015; Koffeman 2015, C.3.6.; Van Sasse van Ysselt 2017, p. 409.

277 EHRM 10 juni 2010, nr. 302/02, ECLI:CE:ECHR:2010:0610JUD000030202 (*Jehovah's Witnesses of Moscow t. Rusland*), *EHRC* 2010/89, m.nt. J.H. Gerards, *GJ* 2010/111 m.nt. A.C. Hendriks.

278 Gerecht 13 september 2013, zaak T-383/11, ECLI:EU:T:2013:431 (*Makhlouf*), *EHRC* 2013/231.

279 Bijv. EHRM 27 maart 2008, nr. 44009/05, ECLI:CE:ECHR:2010:0304JUD004400905 (*Shtukatarov t. Rusland*), *EHRC* 2008/74 m.nt. C. Forder, par. 83.

280 Zie bijv. EHRM 29 maart 2016, nr. 16899/13, ECLI:CE:ECHR:2016:0329JUD001689913 (*Kocherov en Sergeyeva t. Rusland*), *EHRC* 2016/161.

281 EHRM 29 april 2002, nr. 2346/02, ECLI:CE:ECHR:2002:0429JUD000234602 (*Pretty t. het Verenigd Koninkrijk*), *EHRC* 2002/47 m.nt. J.H. Gerards & H.L. Janssen, par. 65; EHRM 20 januari 2011, nr. 31322/07, ECLI:CE:ECHR:2011:0120JUD003132207 (*Haas t. Zwitserland*), *EHRC* 2011/53 m.nt. G. den Hartogh, *NJ* 2002/647 m.nt. J. Legemaate; EHRM 19 juli 2012, nr. 497/09, ECLI:CE:ECHR:2012:0719JUD000049709 (*Koch t. Duitsland*), *EHRC* 2012/220; EHRM 14 mei 2013, nr. 67810/10, ECLI:CE:ECHR:2014:0930JUD006781010 (*Gross t. Zwitserland*), *EHRC* 2013/152 m.nt. A.C. Hendriks; EHRM (GK) 5 juni 2015, nr. 46043/14, ECLI:CE:ECHR:2015:0605JUD004604314 (*Lambert t. Frankrijk*), *EHRC* 2015/171 m.nt. J.H. Gerards; EHRM 27 juni 2017, nr. 39793/17, ECLI:CE:ECHR:2017:0627DEC003979317 (*Gard e.a. t. het Verenigd Koninkrijk*), *EHRC* 2017/193 m.nt. J.H. Gerards.

282 EHRM (GK) 16 december 2010, nr. 25579/05, ECLI:CE:ECHR:2010:1216JUD002557905 (*A., B. en C. t. Ierland*), *EHRC* 2011/40, m.nt. A.C. Hendriks & J.H. Gerards, *NJ* 2011/216 m.nt. E.A. Alkema, *GJ* 2011/36 m.nt. A.C. Hendriks.

283 Zie bijv. EHRM (GK) 10 april 2007, nr. 6339/05, ECLI:CE:ECHR:2007:0410JUD000633905 (*Evans t. het Verenigd Koninkrijk*), *NJ* 2007/459 m.nt. J. de Boer, *EHRC* 2007/73 m.nt. E. Brems, par. 71; zie nader Koffeman 2015, C.3.8.

IVF, vallen onder art. 8 EVRM.[284] Hetzelfde geldt voor de band die wensouders (willen) aangaan met een uit een draagmoeder geboren kind.[285]

23. Kritische of negatief geladen meningsuitingen waardoor iemands *reputatie* of iemands eer en goede naam worden aangetast vormen een inbreuk op art. 8 EVRM.[286] Deze meningsuitingen kunnen het individu raken in hun persoonlijke integriteit en persoonlijke ontwikkeling, aldus het Hof.[287] Kritiek die onderdeel uitmaakt van het publieke debat kan eveneens een inbreuk vormen op iemands reputatie.[288]
24. Het recht op een *gezonde leefomgeving* valt tot op zekere hoogte ook binnen het bereik van art. 8 EVRM. Dat geldt alleen als sprake is van een milieubelasting die het woongenot, het welzijn of de gezondheid van iemand aantast op een 'voldoende ernstige' manier – er moet volgens vaste rechtspraak een zeker 'minimum level of severity' zijn bereikt.[289] Voor het EU-Handvest is het minder nodig om dit recht onder de reikwijdte van art. 7 Hv te brengen, omdat het Handvest een afzonderlijke bepaling bevat over milieubescherming in art. 37 Hv. Deze bepaling heeft vooralsnog echter vooral interpretatieve waarde gehad; het gaat niet om een zelfstandig inroepbaar, subjectief grondrecht.[290]

II.1.5.3 Beperkingsmogelijkheden en positieve verplichtingen

Forum internum – absoluut en niet-beperkbaar

Hiervoor is al aangegeven dat het *forum internum* absolute beperking geniet. De beperkingsclausule van art. 9, tweede lid EVRM geeft alleen de mogelijkheid tot beperking van de vrijheid van belijdenis en van het uiten van godsdienst of overtuiging. De eigenlijke vrijheid van geweten, gedachte en overtuiging wordt hier dus niet genoemd. Iets soortgelijks geldt voor art. 10 EVRM, al vermeldt art. 10, tweede lid EVRM, dit minder duidelijk. Nu art. 10 en 11 Hv corresponderende bepalingen zijn voor art. 9 en 10 EVRM, geldt op grond van art. 52, derde lid Hv dat geen verdergaande beperkingen mogelijk zijn onder het EU-Grondrechtenhandvest dan aanvaardbaar zijn onder het EVRM. Ook al bevat art. 52 lid 1 Hv een algemene, voor alle grondrechtenbepalingen relevante beperkingsclausule, aan-

284 Bijv. EHRM (GK) 3 november 2011, nr. 57813/00 (*S.H. e.a. t. Oostenrijk*), *EHRC* 2012/38 m.nt. B. van Beers, par. 82; EHRM (GK) 10 april 2007, nr. 6339/05, ECLI:CE:ECHR:2007:0410JUD000633905 (*Evans t. het Verenigd Koninkrijk*), *NJ* 2007/459 m.nt. J. de Boer, *EHRC* 2007/73 m.nt. E. Brems.

285 EHRM (GK) 24 januari 2017, nr. 25358/12, ECLI:CE:ECHR:2017:0124JUD002535812 (*Paradiso en Campanelli t. Italië*), *EHRC* 2017/85 m.nt. C. Mak, par. 163.

286 Bijv. EHRM 15 november 2007, nr. 12556/03, ECLI:CE:ECHR:2007:1115JUD001255603 (*Pfeifer t. Oostenrijk*), *EHRC* 2008/6, m.nt. J.H. Gerards. Zie uitgebreid Smet 2010; Smet 2015, C.4.1.1.

287 Idem.

288 Idem.

289 Zie bijv. EHRM 9 juni 2005, nr. 55723/00 ECLI:CE:ECHR:2005:0609JUD005572300 (*Fadeyeva t. Rusland*), *EHRC* 2005/80, m.nt. H.L. Janssen, par. 68-70; zie nader Sanderink 2015.

290 Zie bijv. Greer, Gerards & Slowe 2018, p. 353.

genomen moet daarom worden dat het *forum internum* ook onder het EU-Grondrechtenhandvest absolute bescherming geniet.

Wettelijke grondslag, voorzienbaarheid en bescherming tegen willekeur

De overige privacybepalingen in het Handvest en het EVRM zijn niet absoluut. Voor het EVRM blijkt dit expliciet uit het tweede lid van art. 8 EVRM, voor het Handvest uit art. 52, eerste lid. Anders dan de hiervoor beschreven formeelwettelijke en gespecificeerde beperkingsclausule van art. 10, eerste lid Gw, heeft het vereiste van een wettelijke grondslag in het EVRM en het EU-Grondrechtenhandvest een materieel karakter.[291] Dit betekent dat beperkingen van de privacy voldoende voorzienbaar en toegankelijk moeten zijn en dat ze moeten beschermen tegen willekeur.[292] Dit is in het bijzonder van belang waar het gaat om het toepassen van bevoegdheden tot het plaatsen van verborgen camera's, het afluisteren van telefoons, het plaatsen van GPS-devices, etc. Het uitgangspunt bij het inzetten van dit soort privacybeperkende surveillancemethoden is immers dat de betrokkene niet op de hoogte is van het feit dat hij wordt gevolgd of afgeluisterd; anders zouden de methoden hun doel voorbij schieten. Volgens vaste rechtspraak moeten er in dit soort gevallen wel uitgebreide waarborgen tegen willekeur worden geboden.[293] De regelgeving waarin surveillancebevoegdheden zijn neergelegd, moet zo transparant en kenbaar mogelijk zijn, zodat mensen kunnen inschatten wanneer zij in de gaten worden gehouden.[294] Daarnaast moeten er waarborgen van voorafgaande controle zijn en mogen de bevoegdheden niet zodanig van aard zijn dat zij gemakkelijk kunnen worden misbruikt, bijvoorbeeld doordat ze overmatig ruim zijn geformuleerd.[295] Ten slotte moet in ieder geval achteraf de betrokkene worden ingelicht over het toezicht, zodat deze daartegen eventueel rechtsmiddelen kan instellen.[296] Die rechtsmiddelen moeten dan uiteraard wel beschikbaar zijn.[297]

Deze hoge eisen stellen de rechters overigens niet alleen als het gaat om 'secret surveillance', maar tot op zekere hoogte ook als het gaat om andere maatregelen die vergaande privacyinbreuken veroorzaken. Het gaat dan bijvoorbeeld om doorzoekingen van woningen

291 Zie nader o.m. Gerards 2011, p. 112 e.v.
292 Idem.
293 Zie zeer gedetailleerd EHRM (GK) 4 december 2015, nr. 47143/06 (*Roman Zakharov t. Rusland*), *EHRC* 2016/87 m.nt. M. Hagens, *NJ* 2017/185 m.nt. E.J. Dommering.
294 Idem, par. 239-242.
295 Idem, par. 243 e.v.
296 Idem, par. 286 e.v.
297 Idem.

en kantoorgebouwen,[298] preventief fouilleren[299] of het afnemen van bijvoorbeeld vingerafdrukken.[300]

Noodzakelijkheid en proportionaliteit van beperkingen ter bereiking van een legitiem doel
Privacyrechten kunnen alleen worden ingeperkt als daarmee een legitiem doel wordt nagestreefd. Voor het EU-Grondrechtenhandvest is daarbij een algemeen belang voldoende,[301] het EVRM vereist dat de concrete doelstellingen van een beperking inpasbaar zijn in een van de doelcriteria die in het tweede lid van art. 8 EVRM zijn opgenomen. Het EHRM hecht meestal relatief weinig waarde aan deze doelcriteria. Tenzij duidelijk sprake is van een vorm van détournement de pouvoir of van het verhullen van een niet legitiem doel, accepteert het Hof de meeste doelstellingen als vallend binnen de doelcriteria van het EVRM.[302] Daarnaast vereisen het EVRM en het Hv dat beperkingen van de privacy noodzakelijk en proportioneel zijn ter bereiking van dit doel. Wordt de privacy vergaand aangetast of gaat het om een kernaspect van het recht op privacy, dan zal het EHRM daarbij hoge eisen stellen en niet snel accepteren dat een beperking noodzakelijk en proportioneel is; het gediende maatschappelijk belang moet dan heel zwaarwegend zijn.[303] Van een kernaspect is al snel sprake wanneer een aspect van privacy nauw verband houdt met de menselijke waardigheid of de persoonlijke autonomie – dat is de rol van deze beginselen als 'beperkingsbegrenzer' die in het begin van deze paragraaf al even werd genoemd.[304] Wordt een meer 'perifeer' aspect van het privéleven geraakt, dan is de toetsing meestal minder strikt en laat het Hof meer ruimte voor rechtvaardigingen voor regulering. Het HvJ kiest een soortgelijke benadering door bijvoorbeeld te aanvaarden dat doorzoeking van een commerciële bedrijfsruimte gemakkelijker te rechtvaardigen en sneller toelaatbaar is dan doorzoeking van een woonhuis.[305] Meer ruimte is er daarnaast wanneer er een kwestie moreel of ethisch gevoelig is (zoals abortus) of als er gevoelige overwegingen van veiligheid of sociaal-economische afwegingen aan een privacybeperking ten grondslag

298 Voor een recent voorbeeld, zie EHRM 18 mei 2017, nr. 40927/05, ECLI:CE:ECHR:2017:0518JUD004092705 (*Boze t. Letland*).

299 Zie EHRM 12 januari 2010, nr. 4158/05, ECLI:CE:ECHR:2010:0112JUD000415805 (*Gillan en Quinton t. het Verenigd Koninkrijk*), *EHRC* 2010/30 m.nt. P.B.C.D.F. van Sasse van Ysselt, *NJ* 2010/325 m.nt. E.J. Dommering.

300 Zie EHRM (GK) 4 december 2008, nrs. 30562/04 en 30566/04, ECLI:CE:ECHR:2008:1204JUD003056204 (*S. en Marper t. het Verenigd Koninkrijk*), *EHRC* 2009/13 m.nt. B.J. Koops, *NJ* 2009/410 m.nt. E.A. Alkema en zie HvJ EU 17 oktober 2013, zaak C-291/12, ECLI:EU:C:2013:670 (*Schwarz*), *EHRC* 2014/6 m.nt. D. Groenenberg, *AB* 2014/129 m.nt. A.M. Klingenberg.

301 Zie art. 52, eerste lid Hv.

302 Zie nader Gerards 2011, p. 132 e.v.

303 Zie nader Gerards 2011, p. 215 e.v.

304 Zie voor een klassiek voorbeeld het verbieden van homoseksualiteit: EHRM 22 oktober 1981, nr. 7525/76, ECLI:CE:ECHR:1981:1022JUD000752576 (*Dudgeon t. het Verenigd Koninkrijk*), par. 52.

305 HvJ EU 18 juni 2015, zaak C-583/13 P, ECLI:EU:C:2015:404 (*Deutsche Bahn*), par. 20.

liggen.[306] Wel geldt dat, ook wanneer een ruime 'margin of appreciation' aan de staat wordt toegekend voor het beperken van een grondrecht, het EHRM vaak eisen stelt aan de procedurele waarborgen tegen misbruik van deze beperkingsbevoegdheid.[307] Is de rechterlijke toetsing van de redelijkheid van een beperking bijvoorbeeld niet toereikend, of vindt die plaats aan de hand van andere criteria dan in de rechtspraak van het Hof zijn terug te vinden, dan kan het EHRM alsnog tot de slotsom komen dat het EVRM niet voldoende is gerespecteerd.[308]

Positieve verplichtingen

De privacyrechten die hiervoor zijn besproken, zijn negatief geformuleerde afweerrechten: de staat hoort zich niet te mengen in de individuele keuzevrijheid, de lichamelijke integriteit etc. Tegelijkertijd is er een uitgebreide rechtspraak ontwikkeld waaruit blijkt dat de staat ook tal van positieve verplichtingen heeft om de verschillende grondrechten actief te beschermen. Belangrijk is dat twee hoofdtypen van verplichtingen kunnen worden onderscheiden:[309]

- Enerzijds zijn er *procedurele positieve verplichtingen*. Hiervoor is bijvoorbeeld al gewezen op de verplichtingen om waarborgen te treffen tegen willekeur bij opsporingsbevoegdheden, of op de verplichting om te voorzien in voldoende rechtsmiddelen om op te kunnen komen tegen de aantasting van grondrechten. Deze procedurele positieve verplichtingen zijn voor vrijwel alle in paragraaf II.1.5.2 gedefinieerde rechten in de rechtspraak van het EHRM terug te vinden.[310] Ook in de rechtspraak van het HvJ EU zijn op een aantal plaatsen relevante positieve verplichtingen vastgesteld.[311] In paragraaf II.4 – over procedurerechten – wordt daarop nader ingegaan.
- Anderzijds zijn er *materiële positieve verplichtingen*, die vooral in de rechtspraak van het EHRM zijn ontwikkeld.[312] Daarbij dient de staat bepaalde middelen te verschaffen om de uitoefening van een grondrecht effectief mogelijk te maken. Zo kan de vraag opkomen of de staat bepaalde reproductieve middelen financieel bereikbaar moet maken om het recht op het stichten van een gezin mogelijk te maken, en of de staat actief informatie beschikbaar moet maken om de voor- of nadelen van een medische behandeling in te kunnen schatten. Over deze positieve verplichtingen is een schat aan rechtspraak beschikbaar, waarin voor elk van de hiervoor omschreven deelrechten van

306 Zie, met diverse voorbeelden voor zowel het EHRM als het HvJ EU, Gerards 2011c.
307 Zie voor een willekeurig voorbeeld EHRM 21 november 2017, nr. 47056/11, ECLI:CE:ECHR:2017:1121JUD004705611 (*Panyshkiny t. Rusland*).
308 Idem.
309 Zie veel uitgebreider bijv. Beijer 2017; Lavrysen 2016.
310 Zie voor een overzicht De Jong 2017.
311 Nader Beijer 2017.
312 In de rechtspraak van het HvJ EU zijn dergelijke verplichtingen nauwelijks te vinden, hetgeen veel te maken heeft met de andere institutionele inbedding van het Handvest; zie uitgebreid Beijer 2017.

privacy passende positieve verplichtingen zijn geformuleerd. Deze positieve verplichtingen zijn zeer divers en ze lenen zich niet voor een korte en overzichtelijke opsomming in dit hoofdstuk. Daarvoor zij verwezen naar de relevante gespecialiseerde literatuur over specifieke (deel)onderwerpen.[313] In algemene zin kan wel worden opgemerkt dat het Hof een 'fair balance'-test toepast bij het bepalen welke positieve verplichtingen een staat in een concreet geval heeft. Daarbij bekijkt het vooral of van de staat redelijkerwijs verwacht kan worden dat een bepaalde actie wordt genomen, ook gelet op de belangen die voor de staat zelf op het spel staan.[314] Zo achtte het Hof het niet redelijk om de staat te verplichten om het aantal nachtvluchten op de luchthaven Heathrow te beperken om de omwonenden verdere geluidsoverlast (en de daarmee gepaard gaande inbreuk op hun privéleven) te besparen, onder meer vanwege de economische belangen die gemoeid waren met het door laten gaan van de nachtvluchten.[315] Daarentegen verplichtte het Hof de staat wél om op te treden tegen geluidsoverlast door cafés in een woonwijk, vooral omdat de bevoegde autoriteiten door hun nalatigheid handelden in strijd met hun zelf vastgestelde beleid.[316]

II.1.5.4 Horizontale werking

In het verlengde van de hierboven omschreven positieve verplichtingen, kan het verdragsrechtelijk gecodificeerde grondrecht op privacy ook een belangrijke betekenis hebben voor horizontale rechtsverhoudingen. Deze betekenis komt op verschillende manieren tot uitdrukking:

- In het EU-recht is het mogelijk dat bepaalde aspecten van het recht op privacy nader zijn gereguleerd in EU-wetgeving, waarbij die regelgeving zo is ingericht dat ook particulieren en bedrijven daardoor worden geraakt. Dit is in de praktijk vooral belangrijk waar het gaat om gegevensbescherming, een onderwerp dat in dit onderzoek buiten beschouwing blijft.
- Het EHRM heeft in een groot aantal uitspraken positieve verplichtingen tot regelgeving voor specifieke, particuliere rechtsverhoudingen vastgelegd. Een kenmerkend voorbeeld is dat het Hof weliswaar toelaat dat ook werkgevers inbreuk maken op de privacy van hun werknemers, bijvoorbeeld door inzage te krijgen in hun computerbestanden of door camera's op te hangen, maar dat het Hof dan vereist dat nationale regelgeving

313 Zie in algemene zin voor art. 8 EVRM de al eerder genoemde bronnen: De Vries 2018 en het Sdu Commentaar EVRM (bijv. Koffeman 2015, Smet 2015, Sanderink 2015).

314 Zie nader Lavrysen 2016; Gerards 2011, p. 233.

315 EHRM (GK) 8 juli 2003, nr. 36022/97, ECLI:CE:ECHR:2003:0708JUD003602297 (*Hatton t. het Verenigd Koninkrijk*), *EHRC* 2003/71 m.nt. H.L. Janssen, *AB* 2003/445 m.nt. A. Woltjer, *NJ* 2004/207 m.nt. E.J. Dommering.

316 EHRM 16 november 2004, nr. 4143/02, ECLI:CE:ECHR:2004:1116JUD000414302 (*Moreno Gómez t. Spanje*), *EHRC* 2005/12 m.nt. H.L. Janssen, *NJ* 2005/344 m.nt. E.J. Dommering.

wordt aangenomen om de zorgvuldigheid van dit toezicht te reguleren.[317] Deze nationale regelgeving moet behoorlijk precies zijn en moet ervoor zorgen dat werkgevers waarborgen bieden die sterk vergelijkbaar zijn met de waarborgen die art. 8 EVRM biedt tegen willekeur bij surveillance door de staat. Voorzien moet bijvoorbeeld worden in transparante regelgeving, in een voorafgaande communicatie over de monitoring, en in voldoende toegang tot de rechter.[318] Op een soortgelijke manier heeft het EHRM aangenomen dat een staat een goed stelsel van regelgeving moet introduceren om inbreuken door privépersonen op de lichamelijke of geestelijke integriteit te voorkomen. Het gaat dan zowel om – bijvoorbeeld – strafrechtelijke bescherming tegen verkrachting[319] als om regelgeving om ervoor te zorgen dat artsen en ziekenhuizen zich houden aan de eisen van 'informed consent' bij medisch ingrijpend handelen.[320] Dergelijke regelgeving moet bovendien voldoende effectief worden gehandhaafd.[321] Op deze manier heeft art. 8 EVRM veel betekenis voor horizontale rechtsverhoudingen, al is het indirect. Overigens is in dit verband ook het opmerken waard dat het Human Rights Committee (hierna HRC) van de Verenigde Naties in 1988 in een algemeen commentaar ook een aantal richtlijnen heeft gegeven voor de interpretatie van het privacyrecht zoals dat is neergelegd in art. 17 IVBPR.[322] Het HRC geeft hier uitdrukkelijk in aan dat art. 17 IVBPR horizontale werking moet toekomen en dat het dus ook moet kunnen beschermen tegen inbreuken door natuurlijke en rechtspersonen.[323] Deze horizontale werking dient volgens het HRC vorm te krijgen door middel van wetgeving en andere maatregelen om te verzekeren dat genoemde rechten daadwerkelijk worden beschermd. De staat heeft dus een positieve verplichting om hierin te voorzien, net als onder het EVRM.[324]

– Behalve de wetgever heeft ook de nationale rechter volgens het EHRM een positieve verplichting om in overeenstemming met het EVRM te oordelen, en dus te oordelen in lijn met de vereisten die het EHRM voor art. 8 EVRM heeft geformuleerd. Deze verplichting heeft de rechter ook in kwesties die een privaatrechtelijk karakter hebben. Zo kan de rechter te maken krijgt met een privaatrechtelijke smaadzaak, waarbij iemand schadevergoeding eist vanwege de aantasting van zijn reputatie door een publicatie

317 Zie in het bijzonder EHRM (GK) 5 september 2017, nr. 61496/08, ECLI:CE:ECHR:2017:0905JUD006149608 (*Bărbulescu t. Roemenië*), *EHRC* 2018/3 m.nt. B.P. ter Haar, *JAR* 2017/259 m.nt. C.M. Jakimovicz.

318 Idem.

319 Zie klassiek EHRM 26 maart 1985, nr. 8978/80, ECLI:CE:ECHR:1985:0326JUD000897880 (*X. en Y. t. Nederland*), *NJ* 1985/525 m.nt. E.A. Alkema, *NJCM-Bull.* 1985, p. 410 m.nt. J.G.C. Schokkenbroek.

320 Bijv. EHRM 15 januari 2013, nr. 8759/05, ECLI:CE:ECHR:2013:0115JUD000875905 (*Csoma t. Roemenië*), *EHRC* 2013/81 m.nt. A.C. Hendriks.

321 Uitgebreid daarover, specifiek in verband met de bescherming van een goed milieu, Sanderink 2015.

322 Human Rights Committee, CCPR General Comment No. 16: The right to respect of privacy, family, home and correspondence, and protection of honour and reputation (*Art. 17*), van 8 april 1988.

323 Vgl. De Vries 2013, p. 155.

324 Joseph, Schultz & Castan 2004.

van een journalist. In een dergelijk geval moet de nationale rechter een afweging maken van belangen (reputatiebescherming tegenover vrijheid van meningsuiting), aan de hand van de criteria die daarvoor in de rechtspraak van het EHRM zijn geformuleerd.[325] Ook via deze constructie kan het recht op privacy, in al zijn verschillende aspecten, een grote invloed hebben op horizontale rechtsverhoudingen.

II.2 Gelijkheidsrechten

II.2.1 Rationale en betekenis; aanpak van deze paragraaf

Het recht op gelijke behandeling en non-discriminatie is een complex recht. Bij andere grondrechten, zoals het recht op privacy of de vrijheid van meningsuiting, is het doel duidelijk: het gaat erom de privacy of de meningsuiting zo goed mogelijk te beschermen. Bij gelijke behandeling is het doel lastiger te definiëren. Oneindige gelijke behandeling is zeker niet het streven. Het kan immers wenselijk zijn om te differentiëren tussen mensen of groepen (en hen dus ongelijk te behandelen) om zo goed mogelijk recht te doen aan hun individuele verschillen of wensen. Meestal wordt dan ook aangenomen dat ongelijke behandeling niet als zodanig problematisch is, maar alleen het *zonder goede rechtvaardiging* ongelijk of juist gelijk behandelen van personen of groepen. Zo kan het heel redelijk zijn, en dus niet in strijd met het gelijkheidsbeginsel, om bij hogere inkomensgroepen een hogere inkomensbelasting te heffen dan bij lagere, en kan het gerechtvaardigd of zelfs nodig zijn om bijzondere voorzieningen te treffen om mensen te compenseren die zich in een achterstandspositie bevinden.

Deze complexiteit van de notie van gelijke behandeling maakt dat het lastig is om het 'recht op gelijke behandeling' of het 'recht op non-discriminatie' in wetgeving te vangen. Daar komt nog bij dat er veel verschillende (en minstens zo complexe) concepten zijn die nauw samenhangen met dit recht, zoals directe en indirecte discriminatie. Er zijn dan ook veel gelijkheidscodificaties, die het non-discriminatierecht steeds op een net iets andere manier benaderen en net iets andere aspecten van het recht beschermen. Vanwege deze complexiteit is het nuttig om in deze paragraaf kort stil te staan bij een aantal kernbegrippen en pas daarna in te gaan op de belangrijkste codificaties in verdragen, de Grondwet en wetgeving. Daarbij ligt het accent op die noties die van bijzonder belang zijn in de context van algoritme-gedreven besluitvorming. Achtereenvolgens wordt hierna dan ook aandacht besteed

325 Zie in het bijzonder EHRM (GK) 7 februari 2012, nrs. 40660/08 en 60641/08, ECLI:CE:ECHR:2012:0207 JUD004066008 (*Von Hannover t. Duitsland (nr. 2)*), *EHRC* 2012/72 m.nt. R. de Lange & J.H. Gerards, *NJ* 2013/250 m.nt. E.J. Dommering. Zie over dit voorbeeld nader ook Smet 2010 en Smet 2015.

aan de noties van ongelijke behandeling, rechtvaardiging, discriminatie en 'verdachte' gronden van onderscheid; aan de concepten directe en indirecte discriminatie; aan opzettelijke en onbewuste discriminatie en aan de concepten discriminatie door associatie en discriminatie op veronderstelde gronden. Onderwerpen als positieve discriminatie, segregatie, redelijke accommodatie en intimidatie blijven buiten beschouwing.

II.2.1.1 Ongelijke behandeling, rechtvaardiging, discriminatie en verdachte gronden van onderscheid

(On)gelijke behandeling en benadeling

Een kernelement van het gelijkheidsbeginsel is het feit dat sprake is van een vergelijking tussen twee of meer gevallen, personen of groepen.[326] Veel zaken kunnen op zichzelf worden beschreven – zo kan feitelijk worden vastgesteld dat de Utrechtse Domtoren 112,5 meter hoog is, of dat mevrouw Anders een salaris van 2000 Euro netto per maand verdient. Het is echter ook mogelijk om de beschrijving te geven in vergelijkende termen. Zo kan worden gezegd dat de Utrechtse Dom hoger is dan de Utrechtse Buurkerk, of dat mevrouw Anders een lager nettosalaris verdient dan haar mannelijke collega Meer. In termen van grondrechten is zo'n ongelijke behandeling eigenlijk alleen problematisch als sprake is van een *benadeling* van de ene groep of persoon ten opzichte van de andere, of van het ene geval ten opzichte van het andere.[327] Het is namelijk juist het feit dat iemand nadeel ondervindt van een bepaalde maatregel of een bepaald besluit ten opzichte van iemand anders dat maakt dat er een zekere morele verontwaardiging of een gevoel van oneerlijkheid optreedt, of dat nadeel nu materieel of immaterieel van aard is.[328] Als Anders en Meer hetzelfde verdienen voor gelijke werkzaamheden, is er niet zoveel aan de hand. Maar als Anders minder krijgt, wordt zij daardoor materieel benadeeld; die benadeling vraagt dan om uitleg. Hetzelfde kan gelden als sprake is van een gelijke behandeling van ongelijke gevallen. Stel bijvoorbeeld dat Anders en Meer moeten verhuizen naar een kantoorgebouw dat niet is aangepast voor mensen met een rolstoel, terwijl Meer halfzijdig verlamd is. Anders en Meer worden dan gelijk behandeld, in die zin dat ze beiden moeten verhuizen en beiden in het nieuwe kantoor moeten gaan werken. Meer wordt echter materieel benadeeld ten opzichte van Anders omdat hij vanwege zijn rolstoel dat nieuwe gebouw niet kan betreden en daardoor zijn werk niet kan doen.

Benadeling van de ene persoon of groep ten opzichte van de andere of van het ene geval ten opzichte van het andere, is daarmee het springende punt als het gaat om het gelijkheids-

326 Zie uitgebreid Gerards 2002.
327 Gerards 2002, p. 77.
328 Zie ook Altman 2015.

beginsel. Om die reden zal deze term in dit onderzoek vaak worden gebruikt in plaats van 'gelijke of ongelijke behandeling'.

Vergelijkbaarheid en rechtvaardiging

Het voorgaande laat zien dat het enkele feit dat er een benadeling, nog niet zoveel zegt over de *redelijkheid* of *aanvaardbaarheid* van die benadeling. Aangenomen wordt meestal dat een benadeling redelijk is in twee situaties:

- Er is sprake van een benadeling ten opzichte van elkaar van *onvergelijkbare gevallen of groepen*.[329] Bijvoorbeeld: als hogere premies worden geheven voor de levensverzekering van rokers, kan worden gesteld dat dit redelijk is omdat rokers gemiddeld een lagere levensverwachting hebben dan niet-rokers en deze groepen daardoor significant verschillend zijn. Vanuit het perspectief van levensverwachting zijn de groepen rokers en niet-rokers dus niet vergelijkbaar, zodat een ongelijke behandeling redelijk is. Opgemerkt moet wel worden dat er nogal wat haken en ogen zitten aan deze 'vergelijkbaarheidsbenadering'.[330] Allereerst is het lang niet altijd gemakkelijk om vast te stellen dat groepen of gevallen daadwerkelijk vergelijkbaar of juist verschillend zijn. Daarvoor is het nodig om een vergelijkingsmaatstaf vast te stellen, dus een kenmerk of grond waarop de vergelijking kan worden gebaseerd (in het voorbeeld: roker zijn). Bovendien moet die vergelijkingsmaatstaf relevant en redelijk zijn. Of dat het geval is, hangt af van redelijkheidsoordelen. Zo is het in het voorbeeld de vraag of het redelijk is om 'roken' als relevante vergelijkingsmaatstaf te kiezen bij het vaststellen van premies voor een levensverzekering. Daar kunnen vragen bij worden gesteld als blijkt dat veel mensen er niet zoveel aan kunnen doen dat zij niet van hun rookverslaving afkomen, of als het vergaande consequenties heeft dat rokers een veel duurdere levensverzekering hebben, bijvoorbeeld voor hun mogelijkheid om een hypotheek te nemen.
- Bij de beoordeling van de redelijkheid van een benadeling of bij de beoordeling van de redelijkheid van een vergelijkingsmaatstaf gaat het in juridische termen om de vraag of er een *objectieve en redelijkerechtvaardiging* bestaat voor die benadeling. Dit vereiste van rechtvaardiging kan worden verfijnd naar een aantal concrete criteria:[331]
  1. De *grond* voor het maken van het onderscheid moet voldoende objectief, neutraal en redelijk zijn. Het loutere bestaan van vooroordelen jegens bepaalde groepen is bijvoorbeeld geen neutrale of rationele grond voor het behandelen van die groep

329 Zie nader Gerards 2002, p. 58 e.v.

330 Idem.

331 Zie nader Gerards 2002, p. 679; het hier kort weergegeven model is gebaseerd op een combinatie van rechtstheoretische opvattingen over de eisen die redelijkerwijze aan de rechtvaardiging van benadeling kunnen worden gesteld, en een vergelijkende analyse van het soort eisen dat rechters in de praktijk ook daadwerkelijk aan deze rechtvaardiging stellen. In de praktijk komen niet alle eisen op precies dezelfde manier en even precies aan de orde, maar dit model laat wel zien welke criteria voor het vaststellen van redelijkheid in theorie kunnen gelden.

op een bepaalde manier. Hierna wordt hierop nog verder ingegaan bij het bespreken van 'verdachte' gronden van onderscheid.
2. Er moet een *legitieme doelstelling* bestaan voor het maken van onderscheid tussen twee groepen of gevallen.
3. Een regeling of besluit waarin sprake is van benadeling moet *voldoende specifiek zijn afgebakend* en moet *geschikt* zijn voor het bereiken van het doel. Als het doel van de wetgever voor het toestaan van etnisch profileren bij surveillance bijvoorbeeld is om misdrijven te voorkomen, moet voldoende duidelijk zijn dat de specifieke etnische groepen die nader worden onderzocht daadwerkelijk een groter risico vormen voor misdrijven dan andere groepen.
4. Het moet *noodzakelijk* zijn om voor een bepaalde ongelijke behandeling te kiezen om het nagestreefde doel te bereiken. De vraag is bijvoorbeeld of het doel van het bestrijden van misdrijven ook kan worden bereikt zonder te werken met de methode van etnisch profileren; als dat het geval is, is er geen sterke rechtvaardiging voor deze methode.
5. Er moet een redelijk evenwicht bestaan tussen de individuele of groepsbelangen die worden aangetast door de benadeling (bijvoorbeeld het belang om niet te worden onderworpen aan specifieke surveillancemaatregelen, maar ook het meer immateriële belang om niet te worden buitengesloten) en het doel dat ermee wordt nagestreefd (in dit voorbeeld het bewerkstelligen van een grotere maatschappelijke veiligheid).

Discriminatie en 'verdachte' gronden

Vaak wordt in de context van ongelijke behandeling gesproken van 'discriminatie'. Ongelijke behandeling en discriminatie zijn in de Nederlandse doctrine en in de Nederlandse taal echter geen synoniemen.[332] Het begrip 'discriminatie' heeft een negatieve betekenis, terwijl 'ongelijke behandeling' en 'onderscheid' vrij neutraal zijn. 'Discriminatie' wordt soms gebruikt om aan te duiden dat een benadeling ongerechtvaardigd is. Het begrip vat dan de negatieve uitkomst samen van de hiervoor omschreven rechtvaardigingstoets. Toch is er meestal nog iets meer aan de hand als het begrip 'discriminatie' wordt gebruikt. Het begrip wordt vooral in de mond genomen als een ongelijke behandeling moreel of maatschappelijk verwerpelijk wordt gevonden.[333] Dat is het geval als een benadeling nauw samenhangt met ideeën over inferioriteit van bepaalde groepen of kenmerken, met het historisch of maatschappelijk stigmatiseren en buitensluiten van groepen met bepaalde kenmerken, met vooroordelen of stereotypen, met al te brede generalisaties over wat

332 In de Engelse taal is dat anders; 'discrimination' kan daar juist een neutrale betekenis hebben. Zie uitgebreid over deze problematiek o.m. Holtmaat 2003; Holtmaat 2006.

333 Zie ook Altman 2015; Gerards 2016.

bepaalde mensen kunnen of hoe bepaalde mensen zijn, of als een benadeling wordt gebaseerd op persoonskenmerken die objectief gezien irrelevant zijn voor iemands dagelijkse functioneren in de samenleving.[334]

Voor sommige 'gronden' (= redenen) voor benadeling wordt *a priori* aangenomen dat ze nauw samenhangen met dit soort verwerpelijke motieven. Als Anders bijvoorbeeld een lager salaris krijgt dan Meer omdat zij een vrouw is, ontstaat er automatisch een vermoeden dat dit geen redelijke grond is voor het beloningsverschil. Maatschappelijk gezien wordt 'vrouw zijn' namelijk niet geaccepteerd als rationele rechtvaardiging voor beloningsverschillen, ook al omdat geslacht (in beginsel) niet relevant is voor iemands functievervulling. Anders gezegd: aan dit soort 'gronden' voor onderscheid zit automatisch een luchtje, ze zijn '*verdacht*'.[335]

Belangrijk is dat niet iedere benadeling op een verdachte grond automatisch ongerechtvaardigd is een discriminatie oplevert. Rechtvaardiging is onder meer mogelijk bij zogenaamde 'positieve actie', waarbij bijvoorbeeld vrouwen worden bevoordeeld bij bevordering naar hogere functies om ervoor te zorgen dat er een meer evenwichtige samenstelling van een functiegroep ontstaat. Verdachtheid van een grond van onderscheid is dus vooral een waarschuwingssignaal. Als een benadeling primair is gebaseerd op een verdachte grond, ontstaat het vermoeden dat sprake is van een ongerechtvaardigd onderscheid. Dat vermoeden kan alleen worden weerlegd als er zeer overtuigende en zwaarwegende redenen bestaan voor het maken van dit onderscheid.[336] De eisen die aan de rechtvaardiging op de bovengenoemde criteria worden gesteld, zijn in dat geval aanzienlijk hoger dan normaal.

De vraag rijst daarnaast wanneer een grond 'verdacht' is. Om dat te kunnen bepalen zijn in literatuur en rechtspraak diverse hulpmiddelen aangereikt.[337] In de meeste gevallen gaat het bij 'verdachte' gronden om onderscheid op grond van onveranderlijke persoonskenmerken (zoals huidskleur, etnische afkomst, of geslacht), of om persoonskenmerken waarvan niet in redelijkheid kan worden verwacht dat mensen ze wijzigen (zoals godsdienst of politieke overtuiging). Dit is echter maar één aanwijzing voor de verdachtheid van

334 Zie uitgebreid Gerards 2002, p. 703 e.v.

335 Deze term is ontleend aan de Amerikaanse notie van 'suspect grounds of discrimination'; ook het Europees Hof voor de Rechten van de Mens hanteert deze notie in recentere jaren soms expliciet (bijv. EHRM 15 september 2016, nr. 44818/11, ECLI:CE:ECHR:2016:0915JUD004481811 (*British Gurkha Welfare Society e.a. t. het Verenigd Koninkrijk*), *EHRC* 2016/101 m.nt. J.H. Gerards. Zie voor de ontwikkeling van de notie in de Amerikaanse rechtspraak nader Gerards 2002, p. 475 e.v. en voor de EHRM-ontwikkelingen Gerards 2017a.

336 Het EHRM spreekt in dit verband van een vereiste om 'zeer zwaarwegende redenen' of 'very weighty reasons' als rechtvaardiging aan te voeren; zie nader Gerards 2017a en Gerards 2017b.

337 Zie bijv. Gerards 2002, p. 475 e.v. (met uitvoerige literatuur-/jurisprudentieverwijzingen); Arnardóttir 2014; Loenen 2016; Gerards 2017b (met uitvoerige verwijzingen naar actuele EHRM-rechtspraak).

bepaalde gronden. Belangrijk is ook de algemene irrelevantie van een kenmerk voor het dagelijks functioneren of de 'kwetsbaarheid' van de groep waarvan iemand deel uitmaakt.[338] Voor bepaalde gronden is verder het bestaan van belang van irrationele en sterk gestereotypeerde opvattingen over het typische gedrag van een bepaalde groep, of van historische of maatschappelijke stigmatisering, uitsluiting en achterstelling.[339]

De opvattingen over de 'verdachtheid' van gronden kunnen veranderen. Door maatschappelijke ontwikkelingen kan bijvoorbeeld het besef doordringen dat het in de meeste gevallen niet redelijk is om onderscheid te maken op een bepaalde grond, zoals leeftijd of geboorte, en dat het wenselijk zou zijn om die grond toe te voegen aan het lijstje van verdachte gronden.[340] Ook is er verschil van mening mogelijk over de verdachtheid van bepaalde gronden. Zo zijn sommige gronden wel verdacht in bepaalde contexten, maar niet in andere. Leeftijd is bijvoorbeeld een verdachte grond als het gaat om ontslag van werknemers, maar niet of nauwelijks als het gaat om de vraag wanneer iemand een rijbewijs mag halen of zijn stem mag uitbrengen. Dit maakt dat het niet mogelijk is om een statisch en eenduidig lijstje van verdachte gronden vast te stellen. Eigenlijk moet per situatie worden bekeken of een grond in de gegeven context verdacht is.[341] Niettemin werken veel gelijkheidscodificaties en rechters voor het gemak en voor de duidelijkheid wel met lijsten van verdachte (of zelfs 'verboden') gronden, waarop meestal kenmerken voorkomen als ras, etnische afkomst, nationale afkomst, geslacht, seksuele gerichtheid, burgerlijke staat, geboorte, godsdienst, politieke gezindheid, handicap, chronische ziekte en leeftijd.[342]

II.2.1.2 Directe en indirecte discriminatie

Een begrippenpaar dat in discussies over het recht op non-discriminatie veel wordt gebruikt, is dat van directe en indirecte discriminatie. De relevantie van dit begrippenpaar hangt nauw samen met de hiervoor beschreven verdachtheid van bepaalde onderscheidingsgronden, die maakt dat voor onderscheid op een verdachte grond een extra zware rechtvaardiging moet worden gegeven.[343] In paragraaf II.2.2 wordt bovendien verder beschreven dat sommige codificaties van het gelijkheidsbeginsel een heel specifieke bescherming geven aan ongelijke behandeling die op verdachte gronden is gebaseerd. Dit maakt dat het in de rechtspraktijk heel belangrijk is om aan te tonen dat een ongelijke behandeling daadwerkelijk op één van deze verdachte gronden. Dat is wat meestal als *'directe' discriminatie* wordt aangeduid. Een verdachte grond (bijvoorbeeld ras of geslacht) is dan het enige of

338 Vgl. Timmer 2013.
339 Nader bijv. Timmer 2011.
340 Nader Gerards 2016.
341 Gerards 2016.
342 Zie voor een recente en uitgebreide lijst met name art. 21 Hv; daarin zijn ook gronden opgenomen als sociale afkomst, genetische kenmerken, taal, het behoren tot een nationale minderheid en vermogen.
343 Zie nader bijv. Gerards 2011.

in ieder geval doorslaggevende motief voor een benadeling.[344] Directe discriminatie doet zich bijvoorbeeld voor als een werkgever in een vacature expliciet vermeldt dat hij op zoek is naar een vrouw of dat alleen mensen met de Nederlandse nationaliteit mogen solliciteren.

Directe discriminatie op verdachte gronden is in de praktijk vaak moeilijk aan te tonen.[345] Als een verdacht motief rechtstreeks ten grondslag ligt aan een benadelende beslissing, zal de verantwoordelijke dat meestal niet expliciet zeggen.[346] Een tweede probleem is dat veel vormen van maatschappelijke ongelijke behandeling niet voortvloeien uit bewuste, expliciete beslissingen om bepaalde groepen te benadelen of achter te stellen. Het statistische gegeven dat er relatief gezien minder vrouwen dan mannen in hoge functies in het bedrijfsleven werken, kan bijvoorbeeld maar zelden worden verklaard door bewuste beslissingen van het management om geen vrouwen te benoemen. Het zijn eerder subtiele en moeilijk tastbare maatschappelijke mechanismen die maken dat mannen sneller doorstromen naar hogere functies.[347] Het resultaat (achterstelling van vrouwen) kan in die gevallen problematisch worden gevonden, maar met het concept van directe discriminatie is dat niet goed te bestrijden.

Het concept van *indirecte discriminatie* vormt een belangrijke oplossing voor bewijsproblemen en bij benadeling met maatschappelijke oorzaken.[348] Bij indirecte discriminatie is een benadeling namelijk niet rechtstreeks gebaseerd op een verdachte grond, maar is dit het indirecte effect van een 'neutrale' regeling of beslissing wel dat leden van de groep die zo'n verdachte grond kenmerkt, worden benadeeld. Stel bijvoorbeeld dat een bedrijf besluit om als schoonmaker alleen mensen aan te nemen die Nederlands spreken op B2-niveau. Daarmee baseert het bedrijf het onderscheid op taalbeheersing, wat op zichzelf een niet-verdachte grond is. Tegelijkertijd is duidelijk dat het veel gemakkelijker is om aan deze eis te voldoen voor mensen die in Nederland zijn geboren en opgegroeid dan voor mensen die een andere nationale afkomst hebben. In dit geval kan dan ook worden aangenomen dat sprake is van indirecte discriminatie naar nationale afkomst.

Ook bij indirecte discriminatie kan worden gevraagd om een objectieve en redelijke rechtvaardiging, op dezelfde manier als bij directe vormen van ongelijke behandeling. In het gegeven voorbeeld zal het bedrijf dan moeten uitleggen waarom schoonmakers een

344 Zie nader Bell 2007.

345 Nader Bell 2007.

346 Een bijkomende problematiek is er wanneer sprake is van discriminerende geweldpleging; daarbij is er vaak niet een duidelijk element van ongelijke behandeling, maar wordt een handelen ingegeven door afkeer van een bepaalde groep. Daarbij moet vaak een discriminerend motief worden aangetoond (zie ook hierna, par. II.2.1.3), maar ook dat is in de praktijk bijzonder moeilijk; zie Mačkić 2017.

347 Altman 2015.

348 Zie uitgebreid bijv. Gerards 2002; Tobler 2005; Schiek 2007.

B2-niveau aan Nederlands moeten beheersen, en ook waarom het belang van deze doelstelling opweegt tegen het effect van de regeling (namelijk dat vooral niet-Nederlanders van de functie worden uitgesloten). Vrij algemeen wordt aangenomen dat de aan de rechtvaardiging te stellen eisen ook bij indirecte discriminatie hoger moeten zijn als de benadeling indirect op een verdachte grond is gebaseerd (zoals in het voorbeeld).[349]

Indirecte discriminatie kan in de meeste gevallen worden aangetoond door middel van statistisch bewijs waaruit blijkt welk deel van een als geheel benadeelde groep bestaat uit mensen met een 'verdacht' kenmerk (zoals een bepaald geslacht, een bepaalde huidskleur, een handicap), maar ook ander materiaal of zelfs logica en gezond verstand kunnen hierbij dienstig zijn.[350] Er is nogal wat discussie mogelijk over de vraag wanneer dan sprake is van een 'indirect discriminerend effect'. Meestal wordt daarvoor het nogal vage criterium gebruikt dat de groep die beschikt over een 'verdacht kenmerk' door een besluit of maatregel 'disproportioneel zwaar' of 'overwegend' wordt geraakt.[351] Daarnaast bestaat er het nodige debat over de vraag hoe de referentiegroepen moeten worden geformuleerd.[352] Moet bij het bepalen van disproportionele oververtegenwoordiging van mannen in een bepaalde functiegroep bijvoorbeeld worden vergeleken met dezelfde functiegroep bij andere bedrijven, of met het bedrijf als geheel, of met een gehele bedrijfstak? Meestal is het antwoord op dit soort vragen alleen in concrete casus te geven.

Het verschil tussen directe en indirecte discriminatie is niet altijd even duidelijk. Als in een regeling niet wordt gekozen voor een verdachte grond als nationaliteit als onderscheidingskenmerk, maar een niet-verdachte grond als het hebben van een Nederlands paspoort, is dan sprake van directe of van indirecte discriminatie? Het antwoord op deze vraag is niettemin belangrijk, omdat – zoals opgemerkt – sommige codificaties duidelijk juridisch verschil maken tussen directe en indirecte discriminatie. Directe discriminatie is vaak expliciet verboden; er zijn dan alleen enkele heel precies omschreven omstandigheden waarin een rechtvaardiging bestaat voor een ongelijke behandeling. Voor indirecte discriminatie bestaat vrijwel altijd een ruimere mogelijkheid van rechtvaardiging.[353] Bovendien zijn sommige vormen van directe en intentionele (zie hierna) discriminatie zwaarder strafbaar gesteld dan andere. Voor discriminatie die voortvloeit uit algoritme-gedreven besluitvorming is dit bijzonder relevant, zoals hierna in hoofdstuk III wordt uitgelegd.

---

349 Idem.

350 Idem. Zie voor een voorbeeld van dit laatste bijv. EHRM (GK) 24 mei 2016, nr. 38590/10, ECLI:CE:ECHR:2016:0524JUD003859010 (*Biao t. Denemarken)*, *EHRC* 2016/209 m.nt. K. de Vries, *AB* 2017/179 m.nt. H.J. Simon.

351 Nader Gerards 2002, p. 587 en 676.

352 Gerards 2002, p. 678.

353 Zie over de problemen die hiermee samenhangen nader Gerards 2008; Gerards 2011.

II.2.1.3 Opzettelijke en onbewuste discriminatie; discriminatie bij associatie en discriminatie op vermeende kenmerken

Opzettelijke en onbewuste discriminatie
Hiervoor is uitgelegd dat discriminatie direct of indirect kan zijn gebaseerd op een bepaalde grond. Dit is niet helemaal hetzelfde als opzettelijke discriminatie tegenover onopzettelijke of onbewuste discriminatie. De vuistregel kan zijn dat directe discriminatie meestal ook bewuste en opzettelijke discriminatie behelst. Als een dienstverlener er expliciet voor kiest zijn diensten alleen aan vrouwen aan te bieden, of een werkgever weigert een moslim in dienst te nemen vanwege diens godsdienst, dan valt moeilijk te beweren dat sprake is van een onbewuste benadeling. Een discriminerend motief kan verder aantoonbaar zijn bij geweldpleging of bij bepaalde beledigende en discriminerende uitingen.[354] Voor de praktijk is in dit soort gevallen de problematiek vooral gelegen in de bewijslast en de verdeling daarvan.

Bij indirecte discriminatie is de situatie complexer. Ook daar kan sprake zijn van opzettelijk handelen. In het hiervoor gegeven voorbeeld van een werkgever die alleen schoonmakers met B2-niveau Nederlands wil aanstellen, *kan* het diens bedoeling zijn geweest om geen buitenlanders te hoeven aanstellen en *kan* daar een discriminerend motief achter schuilgaan. In dat soort gevallen kan strafrechtelijke verantwoordelijkheid voor het misdrijf discriminatie op grond van ras bestaan, mits de opzet voldoende kan worden aangetoond.[355] Ook daar spelen de nodige bewijsproblemen. Indirecte discriminatie kan echter ook een onbedoeld effect zijn van maatschappelijke omstandigheden. Zo kan een werkgever met de beste bedoelingen een systeem van prestatiebeloning invoeren, maar kan in de praktijk blijken dat die elementen nadelig uitpakken voor oudere werknemers of werknemers met een fysieke beperking. In die gevallen is het effect doorslaggevend en moet de werkgever een rechtvaardiging bieden voor het hanteren van deze regeling, ook al heeft hij geen op discriminatie gerichte bedoelingen.

Discriminatie door associatie en discriminatie op een vermeende grond
Meestal worden mensen het slachtoffer van discriminatie omdat ze beschikken over een bepaald kenmerk op grond waarvan in beginsel geen onderscheid mag worden gemaakt (bijvoorbeeld een bepaalde etnische afkomst). Het kan echter ook zijn dat iemand niet wordt benadeeld vanwege zijn eigen persoonskenmerken, maar vanwege de kenmerken van iemand waarmee hij in nauw verband staat. In het Engels wordt deze vorm van discri-

354 Zie daarover o.m. Mačkić 2017; Gerards 2017.
355 Zie art. 137g Sr.

minatie aangeduid als 'discrimination by association'.[356] Een voorbeeld van deze vorm van discriminatie is dat waarbij een vader zorg heeft voor een gehandicapt kind en daardoor minder gemakkelijk aan de prestatie-eisen van de werkgever kan voldoen. Als gevolg daarvan ontvangt hij een lagere beloning dan zijn collega's zonder een gehandicapt kind. In die gevallen is nog steeds sprake van nadelige behandeling vanwege handicap, maar dan niet van de werknemer zelf, maar van iemand waarmee die werknemer in nauw verband staat.[357]

Een laatste discriminatieconcept betreft discriminatie op een vermeende grond – 'discrimination by assumption'. Niet ondenkbeeldig is bijvoorbeeld dat iemand wordt benadeeld omdat *gedacht* wordt dat hij een bepaalde geloofsovertuiging heeft of omdat hij een bepaalde ziekte heeft, zonder dat ooit is uitgezocht of aangetoond dat dit echt klopt.[358] Ook in die gevallen moet een rechtvaardiging worden geboden, zeker als het gaat om onderscheid op een verdachte grond – of degene aan wie een bepaald kenmerk wordt toegeschreven daar nu wel of niet echt over beschikt.

II.2.2 Codificaties van het gelijkheidsbeginsel en het recht op non-discriminatie

Het gelijkheidsbeginsel en het recht op non-discriminatie zijn op tal van plaatsen gecodificeerd. Grofweg kan een tweedeling worden gemaakt in brede of open en specifieke of gesloten codificaties.[359]

Brede codificaties

Brede codificaties zijn die waarbij in algemene termen het gelijkheidsbeginsel wordt gedefinieerd en discriminatie 'op welke grond dan ook' wordt verboden. De voor Nederland meest relevante voorbeelden zijn art. 1 Gw, art. 20 en 21 Hv, art. 14 EVRM en art. 26 IVBPR. Bij die codificaties is het vooral aan de rechter om in concrete gevallen te bepalen of sprake is van een benadeling (al dan niet op een verdachte grond) en of daarvoor een rechtvaardiging is te geven. Die rechtvaardiging wordt dan veelal beoordeeld aan de hand van de criteria die hiervoor in 2.1.1 al zijn weergegeven, waarbij geldt dat bij verdachte

356 Zie bijv. Gerards 2007, p. 169.

357 Zie voor daadwerkelijke voorbeelden HvJ 17 juli 2008, zaak C-303/06, ECLI:EU:C:2008:415 (*Coleman*), *EHRC* 2008/108 m.nt. A.C. Hendriks, *NJ* 2008/501 m.nt. M.R. Mok, TRA 2008 m.nt. A. Veldman; EHRM 22 maart 2016, nr. 23682/13, ECLI:CE:ECHR:2016:0322JUD002368213 (*Guberina t. Kroatië*), *EHRC* 2016/130 m.nt. L. Waddington, *AB* 2017/180 m.nt. H.J. Simon.

358 Zie hiervoor bijv. EHRM 28 maart 2017, nr. 25536/14, ECLI:CE:ECHR:2017:0328JUD002553614 (*Skorjanec t. Kroatië*), *EHRC* 2017/132 m.nt. K. Henrard.

359 Zie voor deze terminologie nader Heringa 1999; Gerards 2008.

gronden de eisen aanzienlijk worden aangescherpt. Weliswaar zijn er nuanceverschillen tussen de aanpak die verschillende hoogste rechters kiezen bij de beoordeling van ongelijke behandeling, maar voor het doel van dit onderzoek is dit minder relevant. Belangrijk is verder dat de meeste van deze codificaties specifiek zijn bedoeld om burgers te beschermen tegen ongelijke behandeling door de staat. Het is moeilijk om er directe horizontale werking aan toe te kennen, in die zin dat mensen de bepalingen rechtstreeks kunnen inroepen tegenover een private partij (een werkgever, een onderneming) in een civiele procedure. Zoals ook het geval is voor andere grondrechten, kan er wel indirecte horizontale werking uitgaan van deze bepalingen. Zo kunnen er uit het EVRM positieve verplichtingen voor de rechter voortvloeien om contracten in lijn met het gelijkheidsbeginsel te interpreteren,[360] of voor de wetgever om wetgeving te maken waardoor discriminatie in horizontale rechtsverhoudingen effectief kan worden aangepakt.[361]

Specifieke codificaties

Specifieke codificaties geven met veel grotere precisie aan welke gevallen van benadeling verboden discriminatie opleveren en welke rechtvaardigingen eventueel mogelijk zijn bij directe en indirecte discriminatie.[362] Bovendien kan de wetgever door middel van specifieke codificaties horizontale werking toekennen aan het discriminatieverbod, bijvoorbeeld door expliciet vast te leggen dat dit verbod geldt voor bepaalde private en/of publieke actoren. Specifieke codificaties zijn meestal 'gesloten' in die zin dat ze zich alleen richten op een beperkt aantal gronden van discriminatie (bijvoorbeeld alleen geslacht, of alleen leeftijd) en op een beperkt aantal situaties (bijvoorbeeld alleen op het terrein van de arbeid, en/of bij dienstverlening, en/of bij sociale bescherming). Daarnaast zijn ze 'gesloten' in die zin dat bij directe discriminatie die is gebaseerd op een van de opgenomen gronden, meestal wordt voorzien in een specifieke en limitatief opgesomde lijst van rechtvaardigingsmogelijkheden. Doet een van die rechtvaardigingsmogelijkheden zich niet voor, dan is de ongelijke behandeling verboden. Alleen voor indirecte discriminatie voorzien veruit de meeste specifieke codificaties in een veel meer open mogelijkheid van rechtvaardiging, waarbij vooral moet worden voldaan aan de vereisten die hiervoor in paragraaf II.2.1.1 zijn opgesomd.

Voor Nederland zijn in het bijzonder de volgende specifieke en gesloten codificaties relevant:

360 EHRM 1 juli 2004, nr. 69498/01, ECLI:CE:ECHR:2004:0713JUD006949801 (*Pla en Puncernau t. Andorra*), *EHRC* 2004/87 m.nt. E. Brems, *NJ* 2005/508 m.nt. J. de Boer.

361 EHRM 6 november 2012, nr. 47335/06, ECLI:CE:ECHR:2012:1106JUD004733506 (*Redfearn t. het Verenigd Koninkrijk*), *EHRC* 2013/29 m.nt. F. Laagland.

362 Zie uitgebreid Gerards 2008.

- Specifieke internationale verdragen als het Verdrag tot uitbanning van alle vormen van rassendiscriminatie ('CERD'), het Verdrag tot uitbanning van alle vormen van discriminatie tegen vrouwen ('CEDAW') en het VN-Verdrag inzake de rechten van personen met een handicap ('UNPD').[363] Deze verdragen richten zich op specifieke gronden van discriminatie, maar ze zijn niet bijzonder gesloten als het gaat om hun bereik en rechtvaardigingsmogelijkheden. De verdragen betreffen alle of een groot aantal terreinen van het maatschappelijk leven en ze bevatten niet altijd even concrete gronden voor rechtvaardiging. Ze hebben maar zelden directe horizontale werking, maar bevatten vooral inspanningsverplichtingen voor de staat om discriminatie tegen te gaan. Veel bepalingen uit dit soort verdragen zijn niet een ieder verbindend, maar ze stellen wel belangrijke kaders voor wetgeving en beleid. In enkele gevallen kan bovendien wel degelijk rechtstreekse werking worden aangenomen.[364]
- Het EU-Grondrechtenhandvest bevat naast de hierboven genoemde brede codificaties ook enkele specifieke verboden van discriminatie, onder meer op grond van handicap, geslacht en leeftijd (zie art. 22-26 Hv). Daarnaast bevat het EU-recht tal van normen die directe en indirecte discriminatie op grond van nationaliteit verbieden, zowel in algemene zin (art. 18 VWEU) of bij het vrij verkeer van personen (art. 45 VWEU), en die gelijke behandeling voorschrijven van EU-burgers (vgl. art. 9 VEU).[365]
- De Algemene wet gelijke behandeling (AWGB) verbiedt directe en indirecte discriminatie op grond van godsdienst, levensovertuiging, politieke gezindheid, ras, geslacht, nationaliteit, hetero-of homoseksuele gerichtheid en burgerlijke staat op het terrein van de arbeid (zowel de publieke als de private sector) en bij het aanbieden van goederen en diensten (inclusief onderwijs). De AWGB dient mede als implementatie van (onder meer) de EU-richtlijnen 2000/43,[366] 2000/78[367] en 2004/113.[368] De eerste van deze twee richtlijnen verbiedt discriminatie op grond van ras (en daaraan gerelateerde gronden) bij de arbeid en bij sociale bescherming; de tweede verbiedt discriminatie op grond van godsdienst of overtuiging, handicap, leeftijd of seksuele geaardheid. Al deze regelingen kenmerken zich door een verbod van directe discriminatie op de genoemde gronden, waarbij een limitatief aantal uitzonderingen mogelijk is. Voor indirecte discriminatie geldt een open mogelijkheid van rechtvaardiging.[369]

---

363 Zie nader Barkhuysen, Van Emmerik & Gerards 2013.

364 Idem.

365 Zie nader bijv. Schiek & Chege 2009.

366 Richtlijn 2000/43/EG van de Raad van 29 juni 2000 houdende toepassing van het beginsel van gelijke behandeling van personen ongeacht ras of etnische afstamming, Pb L 180 van 19/07/2000, p. 22-26.

367 Richtlijn 2000/78/EG van de Raad van 27 november 2000 tot instelling van een algemeen kader voor gelijke behandeling in arbeid en beroep, Pb L 303 van 02/12/2000, p. 16-22.

368 Richtlijn 2004/113/EG van de Raad van 13 december 2004 houdende toepassing van het beginsel van gelijke behandeling van mannen en vrouwen bij de toegang tot en het aanbod van goederen en diensten, Pb L 373 van 21 december 2004, p. 37-43.

369 Zie art. 2 lid 1 AWGB; zie nader o.m. Gerards 2011.

- De Wet gelijke behandeling op grond van leeftijd bij de arbeid (WGBL) betreft, zoals de naam al aangeeft, alleen discriminatie op grond van leeftijd op het terrein van de arbeid. Deze wet vormt een implementatie van de al genoemde EU-richtlijn 2000/78. Deze wet kent grofweg dezelfde systematiek als de AWGB, maar biedt ook bij directe discriminatie een open mogelijkheid van rechtvaardiging.
- De Wet gelijke behandeling op grond van handicap en chronische ziekte (WGBH/CZ) richt zich centraal op discriminatie op grond van handicap en chronische ziekte en vormt mede een implementatie van Richtlijn 2000/78 en van de UNPD. Dit is een aanbouwwet die aanvankelijk alleen op de arbeid betrekking had, maar die inmiddels ook ziet op het aanbieden van goederen en diensten (inclusief het openbaar vervoer). Net als de AWGB bevat deze wet een verbod van directe discriminatie met een beperkt aantal limitatief opgesomde uitzonderingsgronden, en een open mogelijkheid van rechtvaardiging bij indirecte discriminatie.
- De Wet gelijke behandeling van mannen en vrouwen (WGB M/V) is een vroege codificatie van het verbod van discriminatie op grond van geslacht bij de arbeid (zowel de openbare als de private sector) en implementeert onder meer een aantal specifieke EU-richtlijnen die betrekking hebben op gelijke behandeling op grond van geslacht.[370] De bepaling bevat enkele meer specifieke regels in vergelijking tot de AWGB, zoals bepalingen over de vermelding van m/v in vacatureteksten.
- De Wet onderscheid arbeidsduur (WOA) verbiedt ongelijke behandeling van parttimers ten opzichte van fulltimers en de Wet onderscheid bepaalde en onbepaalde tijd (WOBOT) is gericht op gelijke behandeling van mensen met een vast en een tijdelijk arbeidscontract. Beide wetten vormen implementaties van EU-richtlijnen. Ze laten een open rechtvaardigingsmogelijkheid, ook bij direct onderscheid.
- In het Wetboek van Strafrecht zijn enkele specifieke bepalingen terug te vinden waarin discriminatie verboden wordt gesteld. Veelal gaat het daarbij om de uitwerking van verplichtingen die uit specifieke internationale verdragen voortvloeien, zoals het al genoemde CERD. Art. 90quater Sr bevat de definitie van strafrechtelijk verboden discriminatie, die zowel opzettelijke als niet-opzettelijke discriminatie omvat.[371] Art. 429quater Sr stelt discriminatie in de uitoefening van ambt, beroep of bedrijf strafbaar als overtreding wanneer de discriminatie is gebaseerd op ras, godsdienst of levensovertuiging, geslacht of seksuele geaardheid. Art. 137g bevat een soortgelijk verbod voor opzettelijke discriminatie op grond van ras; in dat geval is sprake van een misdrijf.

370 Zie daarvoor de wetsgeschiedenis van deze wet en de wijzigingen die erin in de loop van de tijd zijn doorgevoerd.

371 De definitie luidt: 'Onder discriminatie of discrimineren wordt verstaan elke vorm van onderscheid, elke uitsluiting, beperking of voorkeur, die ten doel heeft of ten gevolge kan hebben dat de erkenning, het genot of de uitoefening op voet van gelijkheid van de rechten van de mens en de fundamentele vrijheden op politiek, economisch, sociaal of cultureel terrein of op andere terreinen van het maatschappelijk leven, wordt teniet gedaan of aangetast.'

Datzelfde geldt voor art. 137a tot en met f; daarbij gaat het onder meer om bepalingen die opzettelijke belediging op grond van ras, godsdienst, levensovertuiging, geslacht of seksuele geaardheid verbieden, die een verbod stellen op het aanzetten tot haat tegen bevolkingsgroepen die over deze kenmerken beschikken, of die deelname aan activiteiten gericht op discriminatie strafbaar stellen.

II.3 Vrijheidsrechten

II.3.1 Inleiding

In paragraaf II.1 is ingegaan op een specifieke set van nauw met de persoonlijke autonomie en menselijke waardigheid verbonden rechten. Vanwege de sterke relatie met de individuele vrijheid worden 'privacyrechten' vaak gezien als onderdeel van de vrijheidsrechten, die veelal worden onderscheiden van gelijkheidsrechten (paragraaf II.2) en procedurele rechten (paragraaf II.4). Nu privacyrechten zo'n belangrijke rol spelen in relatie tot het onderwerp van dit onderzoek en het gaat om een complex stelsel van rechten, is ervoor gekozen ze niet als onderdeel van het cluster 'vrijheidsrechten' te behandelen, maar er een afzonderlijke paragraaf aan te wijden. De onderhavige paragraaf kan zich daardoor concentreren op een andere set van rechten die nauw verband houden met de individuele vrijheid en de individuele ontplooiingsmogelijkheden. Uitgangspunt is dat iedereen het recht moet hebben om zijn overtuigingen, gevoelens en meningen onder woorden te brengen en die te delen met anderen. Dat kan gebeuren in woord of in geschrift, maar ook in de vorm van samenkomsten of protestacties. Daarnaast is het voor iedereen van belang om de vrijheid te hebben om gelijkgestemden op te zoeken en in verenigingsverband samen te komen, of dat nu is met een duidelijk maatschappelijk doel (zoals het geval is bij politieke partijen of vakverenigingen) of vanwege de gezelligheid.

Actieve bescherming van deze vrijheden maakt dat mensen zichzelf kunnen zijn en dat ze – alleen of samen met anderen – uitdrukking kunnen geven aan wat ze belangrijk vinden.[372] Deze rechten dragen bovendien niet alleen bij aan een mogelijkheid tot zelfverwezenlijking en zelfontplooiing. Een aantal van deze rechten is ook van bijzonder belang in een democratische rechtsstaat.[373] Voor een goed functionerende democratische rechtsstaat is het essentieel dat mensen effectief kunnen participeren in het proces dat leidt tot het vaststellen van normen die voor iedereen gelden.[374] Voor die effectieve participatie is noodzakelijk dat mensen vrije toegang hebben tot informatie en dat zij informatie en

372 Vgl. bijv. Nieuwenhuis 2013a, p. 91.
373 Zie nader o.m. Van Sasse van Ysselt 2017b, par. 1.4.
374 Idem.

meningen met elkaar kunnen delen. Vrijheid van meningsuiting en demonstratie zijn dan ook centrale voorwaarden om te kunnen spreken van een democratische rechtsstaat.[375] Daarnaast spelen politieke partijen en politieke bewegingen een belangrijke rol in deliberatieve, representatieve democratieën als de Nederlandse. De verenigingsvrijheid is wezenlijk voor het vrije functioneren van dergelijke partijen en bewegingen. Tot slot is voor het goed functioneren van een democratie essentieel dat er een recht bestaat op deelname aan vrije en geheime verkiezingen voor diegenen die de bevolking representeren in wetgevende (en soms uitvoerende) organen.

Gelet op de nauwe verbanden tussen de verschillende vrijheidsrechten is het nuttig ze in één paragraaf te bespreken. Daarbij wordt hierna aan de verschillende vrijheidsrechten afzonderlijk aandacht besteed. Per vrijheid wordt eerst kort ingegaan op de belangrijkste codificaties van deze vrijheidsrechten en op hun reikwijdte, waarna wordt toegelicht wat de belangrijkste mogelijkheden tot regulering en beperking zijn en welke verplichtingen de staat heeft om deze rechten actief te beperken. Waar relevant wordt ook ingegaan op de horizontale werking van deze vrijheden.

II.3.2 Vrijheid van meningsuiting en vrijheid om informatie te ontvangen

II.3.2.1 Codificaties en reikwijdte

Codificaties

Het recht op vrijheid van meningsuiting omvat verschillende aspecten. Allereerst is er de vrijheid om een mening te *koesteren*. Dit is een recht dat vergelijkbaar is met de gewetensvrijheid, besproken in paragraaf I.1 van dit hoofdstuk over privacyrechten. Dit recht komt hierna dan ook niet verder aan de orde. Belangrijker voor deze paragraaf is de eigenlijke uitingsvrijheid: de vrijheid om gedachten, meningen en gevoelens onder woorden te brengen, in woord of in geschrift. Dit recht is op tal van plaatsen gecodificeerd. In verdragen is het te vinden in art. 19 IVBPR, art. 10 EVRM en art. 11 Hv; in de Grondwet is het terug te vinden in art. 7. Het tweede lid van art. 11 Hv stelt bovendien dat de vrijheid en de pluriformiteit van de media worden geëerbiedigd. Hetzelfde geldt voor artikel 19 IVBPR.[376]

Het uiten van meningen, gedachten of gevoelens is alleen nuttig als die informatie ook door anderen kan worden ontvangen. De vrijheid om informatie te ontvangen wordt meestal dan ook gezien als een noodzakelijk complement van de vrijheid van meningsuiting. Dit komt expliciet tot uitdrukking in art. 10 EVRM, dat volgens het eerste lid de vrijheid

375 Zie nader onder meer AIV 2017, p. 17 e.v.

376 Deze bepaling is wel iets anders geformuleerd en is ook uitgebreider, maar voor het doel van deze paragraaf is dat minder relevant.

omvat om inlichtingen of denkbeelden te ontvangen of te verstrekken. Ook art. 11 Hv geeft aan dat de vrijheid van meningsuiting de vrijheid omvat om een mening te hebben en de vrijheid om kennis te nemen en te geven van informatie of ideeën. Art. 7 Gw omvat dit recht niet; deze bepaling beschermt alleen de eigenlijke openbarings- en verspreidingsvrijheid.[377]

Reikwijdte: uitingsvrijheid

De uitingsvrijheid wordt – zeker in de rechtspraak van het EHRM – ruim gedefinieerd.[378] Het eigenlijke uiten is wat centraal staat, de drager van de uiting is verder niet zo relevant. Of nu sprake is van een klassiek stuk in een krant, van een mening op een webforum, van een tweet of van het dragen van een symbool: in alle gevallen is sprake van een meningsuiting.[379] Er zijn maar een paar beperkingen van de reikwijdte geformuleerd. Zo heeft het EHRM aangenomen dat pure scheldwoorden geen meningsuiting vormen.[380] Daarnaast zijn er enkele uitspraken waaruit kan worden afgeleid dat sterk haatzaaiende uitingen, ontkenning van de holocaust of uitingen die rechtstreeks oproepen tot geweld of intolerantie, niet worden gezien als beschermde uitingen.[381] Voor de Grondwet geldt dat handelsreclame (commerciële uitingen) buiten de reikwijdte van de vrijheid van meningsuiting valt. Het EVRM en het EU-Grondrechtenhandvest dienen hier als vangnet; deze beide bepalingen beschermen commerciële uitingen wel.[382]

Reikwijdte: informatievrijheid

Zoals opgemerkt in paragraaf II.3.2.1 omvatten verschillende codificaties het recht om informatie en denkbeelden te ontvangen.[383] Daarbij wordt vaak een onderscheid gemaakt tussen passieve en actieve informatieontvangst. Bij passieve informatieontvangst gaat het om de vrijheid om kennis te nemen van informatie die door anderen actief wordt geuit –

377 De Staatscommissie Grondwet stelde in 2010 voor om deze lacune door een andere formulering van de tekst op te vangen; zie Staatscommissie Grondwet 2010, p. 71 en 77-78.

378 Ogenschijnlijk is de grondwettelijke bescherming beperkter, nu alleen de openbaringsvrijheid expliciet in art. 7 Gw is terug te vinden; de vrijheid om uitingen te verspreiden is echter in de rechtspraak erkend als een connex recht. Zie nader Nieuwenhuis 2013a, p. 92.

379 Zie nader, met talrijke rechtspraakverwijzingen, Gerards 2017c, C.1.1, Nieuwenhuis 2013a, p. 72.

380 EHRM 2 oktober 2012 (ontv.), nr. 57942/10, ECLI:CE:ECHR:2012:1002DEC005794210 (*Rujak t. Kroatië*), *EHRC* 2013/21 m.nt. A. Nieuwenhuis.

381 Voor nadere analyses en rechtspraakverwijzingen, zie o.m. Gerards 2017c, C.1.5.2; De Morree 2016; Nieuwenhuis 2013a, p. 75-76.

382 Al wordt er minder bescherming aan toegekend als het gaat om puur commerciële reclame, vooral in de rechtspraak van het EHRM; zie nader Gerards 2017c, C.4.1.6.

383 Denk in dit verband ook om de (informatiegaring bij verkiezingen en het gevaar van micro-targeting (beïnvloeden van (groepen) kiezers), vgl. Staatscommissie parlementair stelsel 2017, p. 49 en 50.

bijvoorbeeld televisieuitzendingen, sms-berichten of theatervoorstellingen.[384] Bij actieve informatieontvangst gaat het erom dat mensen het recht hebben om actief toegang te zoeken tot bepaalde informatie. Te denken is dan aan het verkrijgen van toegang tot informatie die in handen is van de overheid of van derden en die de betrokken organisatie niet zelf actief heeft verspreid. Het EHRM neemt aan dat ook het actieve garingsrecht tot op zekere hoogte binnen het bereik van art. 10 EVRM komt, maar alleen voor diegenen die belang hebben bij deze toegang om de informatie daarna actief te kunnen verspreiden.[385] Daarbij kan worden gedacht aan journalisten, maar ook aan belangenbehartigingsorganisaties of activisten.[386] Een algemeen recht op actieve toegang tot informatie dat correspondeert met een verplichting voor de overheid om die informatie te verstrekken, is vooralsnog niet erkend.[387]

II.3.2.2 Beperkingen en verplichtingen

De vrijheid van meningsuiting kan volgens art. 7 Gw alleen door formele wetgeving worden beperkt als het gaat om schriftelijke uitingen; andersoortige uitingen kunnen ook bij lagere regelgeving worden beperkt. Art. 7 Gw is daarbij vooral bijzonder omdat het een vergaand verbod op preventieve beperkingen ('verbod van voorafgaand verlof') omvat, dat bijvoorbeeld ook in de weg staat aan het inrichten van een vergunningenstelsel voor uitgevers of journalisten.[388] Daarnaast kunnen lagere regelgevers grenzen stellen aan het gebruik van bepaalde middelen om informatie te verspreiden, zoals aan het plakken van affiches.[389] Inhoudelijke criteria voor de regulering van de vrijheid van meningsuiting bevat de Grondwet niet.

Dergelijke inhoudelijke criteria voor de mogelijkheden tot regulering en beperking van de vrijheid van meningsuiting en de informatievrijheid zijn wel te vinden in de rechtspraak van het EHRM en in mindere mate van het HvJ EU.[390] Het EHRM heeft daarbij steeds het grote belang van de vrijheid van meningsuiting in een democratische

384 Vgl. bijv. EHRM 16 december 2008, nr. 23883/06, ECLI:CE:ECHR:2008:1216JUD002388306 (*Khurshid Mustafa en Tarzibachi t. Zweden*), *NJ* 2010/149, m.nt. E.A. Alkema, *AB* 2009/286, m.nt. T. Barkhuysen & M.L. van Emmerik, *EHRC* 2009/17 m.nt. J.H. Gerards.

385 EHRM (GK) 8 november 2016, nr. 18030/11, ECLI:CE:ECHR:2016:1108JUD001803011 (*Magyar Helsinki Bizottság t. Hongarije*), *EHRC* 2017/36 m.nt. T. McGonagle, par. 156. Zie uitgebreid Gerards 2017c, C.1.2.

386 Idem.

387 Gerards 2017c, C.1.2; de rechtspraak hierop is verduidelijkt in de al aangehaalde zaak EHRM (GK) 8 november 2016, nr. 18030/11, ECLI:CE:ECHR:2016:1108JUD001803011 (*Magyar Helsinki Bizottság t. Hongarije*), *EHRC* 2017/36 m.nt. T. McGonagle, par. 156, met nadere uitwerking in par. 158-170. Zie recenter ook EHRM 7 februari 2017, nr. 63898/09, ECLI:CE:ECHR:2017:0207JUD006389809 (*Bubon t. Rusland*), *EHRC* 2017/89.

388 Nieuwenhuis 2013a, p. 96.

389 Nieuwenhuis 2013a, p. 97.

390 Het HvJ EU volgt in zijn rechtspraak op dit punt vooral de criteria die het EHRM al heeft ontwikkeld; zie voor het EU-Grondrechtenhandvest, met rechtspraakverwijzingen, o.m. Nieuwenhuis 2013a, p. 90 en Greer, Gerards & Slowe 2018, p. 337.

samenleving vooropgesteld.[391] Zeker als uitingen bijdragen aan discussies over onderwerpen van algemeen belang, kunnen beperkingen alleen worden gesteld als daarvoor een zeer overtuigende en objectieve rechtvaardiging bestaat.[392] Uitingen moeten ook worden toegestaan als ze (voor sommigen) schokkend, storend of beledigend zijn.[393] Een 'chilling effect' moet worden voorkomen; beperkingen, schadevergoedingen of sancties mogen niet zodanig zijn dat mensen erdoor worden ontmoedigd om hun mening naar buiten te brengen.[394]

Staan uitingen in een iets minder direct verband met kernwaarden als democratie, autonomie en menselijke waardigheid – zoals het geval kan zijn bij commerciële uitingen zoals handelsreclame of bij oorlogspropaganda – dan zijn beperkingen volgens de EHRM- en HvJ-rechtspraak gemakkelijker te stellen. Recent heeft het Gerecht van de EU bovendien bepaald dat pure propaganda evenmin wordt beschermd door de vrijheid van meningsuiting.[395] Dat geldt ook wanneer beperkingen worden gesteld met het oog op het beschermen van zwaarwegende maatschappelijke belangen, zoals nationale veiligheid, of wanneer sprake is van een botsing tussen de vrijheid van meningsuiting en de rechten van anderen, zoals het recht op respect voor de eer en goede naam of het non-discriminatierecht.[396] Wel moet in dergelijke gevallen altijd een deugdelijke belangenafweging worden gemaakt, waarbij rekening wordt gehouden met factoren als de ernst en de aard van een beschuldiging of belediging en de positie van degene die is benadeeld.[397]

De uitings- en informatievrijheid is een klassiek grondrecht, dat vooral beschermt tegen actief ingrijpen door de overheid – denk aan overheidscensuur, het verplicht instellen van internetfilters, het vervolgen van journalisten of het actief weghouden van bepaalde informatie voor het grote publiek. De rechtspraak over deze vrijheid laat echter zien dat in de loop van de tijd ook een groot aantal verplichtingen voor de staat is aangenomen om deze vrijheid actief te beschermen.[398]

---

391 Zie uitgebreid Gerards 2017c, C.4.1.

392 Zie klassiek EHRM 7 december 1976, nr. 5493/72, ECLI:CE:ECHR:1976:1207JUD000549372 (*Handyside t. het Verenigd Koninkrijk*), par. 41 en EHRM 26 april 1979, nr. 6538/74, ECLI:CE:ECHR:1979:0426 JUD000653874 (*Sunday Times t. het Verenigd Koninkrijk*), par. 65; zie nader Gerards 2017c, C.4.1.1.

393 *Sunday Times* (zie vorige noot), par. 65.

394 Zie uitgebreid Gerards 2017c, C.5.4.11.

395 Zie voor oorlogspropaganda bijv. Gerecht EU 15 juni 2017, zaak T-262/15, ECLI:EU:T:2017:392 (*Kiselev*), *EHRC* 2017/154 m.nt. P.E. de Morree. Vgl. ook art. 20 IVBPR, dat bepaalt dat alle vormen van oorlogspropaganda en propaganda die aanzet tot haat, discriminatie of geweld moet worden verboden. Zo zijn beperkingen sneller toegestaan als het gaat om pure nieuwsgierigheidsbevrediging of als de uitingen betrekking hebben op privépersonen (in plaats van bijvoorbeeld politici of beroemdheden); zie nader hierover, met tal van bronvermeldingen, Gerards 2017c, C.4.2.

396 Zie uitgebreid Gerards 2017c, C.5.

397 Zie nader o.m. Gerards 2017c, C.5; Nieuwenhuis 2013a.

398 Zie uitgebreid Gerards 2017c, C.3.2.; Nieuwenhuis 2013a, p. 87 e.v.

Gewezen is in dit verband al op de rechtspraak over informatiegaring, waarbij de overheid in een aantal gevallen verplicht is om actief informatie beschikbaar te maken. Dat moet in ieder geval gebeuren als 'waakhonden' als journalisten die informatie willen gebruiken om bepaalde misstanden aan de kaak te stellen.[399] Meer algemeen moet de overheid ervoor zorgen dat mensen toegang hebben via radio en televisie tot onpartijdige en precieze informatie en tot een brede waaier van meningen en commentaren die onder meer de diversiteit van politieke opvattingen in een staat representeert.[400] Publieke media moeten daarbij voldoende voorzien in onafhankelijke en evenwichtige nieuwsvoorziening.[401] Verder moet monopolievorming in de media (ook de commerciële media) worden tegengegaan.[402] De overheid moet bescherming bieden aan journalisten of andere verspreiders van nieuws wanneer zij concreet worden bedreigd door derden.[403] Meer algemeen moet de staat een klimaat creëren dat ruimte biedt voor een open uitwisseling van gedachten en meningen en waarin niemand bang hoeft te zijn voor de consequenties van zijn inbreng.[404]

II.3.2.3 Horizontale werking

De vrijheid van meningsuiting beschermt primair tegen handelen van de overheid. Dat betekent dat bijvoorbeeld redacteuren die bepaalde artikelen weigeren te plaatsen of uitgeverijen die boeken niet willen uitgeven, niet in strijd handelen met de vrijheid van meningsuiting. Zij hoeven die vrijheid immers niet actief te garanderen, zoals de overheid dat wel moet doen.[405] Toch is een zekere verantwoordelijkheid aangenomen van private actoren, die door de overheid kan worden afgedwongen. In dit soort gevallen is geen sprake van strikte horizontale werking. De eisen aan het handelen van bedrijven of personen worden hier immers niet zozeer gesteld door particuliere derde partijen, maar door de overheid. Niettemin is duidelijk dat deze eisen rechtstreeks gevolgen hebben voor de relatie tussen private bedrijven en individuen onderling. Meest evident zijn beperkingen die een nationale rechter oplegt als iemand door bepaalde uitingen een derde heeft beledigd, gediscrimineerd of besmaad. Dergelijke beperkingen kunnen de vorm hebben van een civielrechtelijke boete of rectificatieplicht, maar ook van een strafrechtelijke sanctie. Ze

399 EHRM (GK) 8 november 2016, nr. 18030/11, ECLI:CE:ECHR:2016:1108JUD001803011 (*Magyar Helsinki Bizottság t. Hongarije*), *EHRC* 2017/36 m.nt. T. McGonagle, par. 156.

400 EHRM 17 september 2009, nr. 13936/02 ECLI:CE:ECHR:2009:0917JUD001393602 (*Manole e.a. t. Moldavië*), par. 101-107. Zie nader Gerards 2017c, C.3.2.

401 Idem.

402 EHRM (GK) 7 juni 2012, nr. 38433/09 (*Centro Europa 7 S.r.l. en Di Stefano t. Italië*), *EHRC* 2012/188, m.nt. J. Wolswinkel.

403 Bijv. EHRM 14 september 2010, nrs. 2668/07 e.a. (*Dink t. Turkije*), *NJ* 2012/32 m.nt. E.J. Dommering, *EHRC* 2010/137 m.nt. R. van de Westelaken. Zie Gerards 2017c, C.3.2.

404 Idem; zie Gerards 2017c, C.3.2.

405 Zie bijv. EHRM 16 juli 2013, nr. 1562/10, ECLI:CE:ECHR:2013:0716JUD000156210 (*Remuszenko t. Polen*), par. 79 e.v.

hebben bijvoorbeeld tot doel het non-discriminatierecht, de eer of goede naam of het portretrecht van een derde te beschermen. Bij het doen van uitingen moet een particulier rekening houden met dit soort beperkingen.[406]

Een lastige situatie kan zich voordoen als individuen hun mening willen uiten op webfora of sociale media, die worden beheerd door particuliere bedrijven. Het EHRM heeft aangenomen dat van beheerders van webfora mag worden verwacht dat zij bepaalde uitingen weigeren als die haat zaaien of oproepen tot geweld. Hoewel het Hof expliciet onderkende dat dit soort filterverplichtingen kan leiden tot een vorm van 'private censuur', oordeelde het dat dit de enige manier kan zijn om individuen en groepen effectief tegen schadelijke uitingen te beschermen.[407] Ook kan het zijn dat een postbedrijf niet mag weigeren bepaalde reclamezendingen te versturen omdat het bedrijf het niet eens is met de inhoud daarvan.[408] Dit soort verplichtingen kent tegelijkertijd grenzen. Zo heeft het HvJ bepaald dat van internet service providers niet zonder meer mag worden verwacht dat zij aantastingen van het auteursrecht te voorkomen door filters in te stellen, wanneer daardoor de toegang tot informatie voor individuen wordt beperkt.[409]

Ten aanzien van de vrijheid om informatie te ontvangen, is er in de EHRM-rechtspraak minder duidelijkheid over de vraag of die ook kan worden beperkt door particuliere spelers, bijvoorbeeld doordat informatie alleen in vooraf gefilterde of geselecteerde vorm wordt doorgegeven.[410] Het ligt echter in de lijn der verwachting dat dergelijke rechten en verplichtingen in de toekomst worden aangenomen, gelet op de rechtspraak over de horizontale werking van de uitingsvrijheid als zodanig.

II.3.3 Godsdienstvrijheid

II.3.3.1 Codificaties en reikwijdte

De godsdienstvrijheid kent – net als de vrijheid van meningsuiting – verschillende aspecten. Waar de vrijheid van meningsuiting ook de vrijheid omvat om een mening te koesteren (zonder die te uiten), omvat de godsdienstvrijheid ook de gewetensvrijheid en het recht

406 Zie hierover aan de hand van de EHRM-rechtspraak uitgebreid Gerards 2017c, C.5; voor Nederland, zie o.m. Nieuwenhuis 2013a, p. 97-98.

407 EHRM (GK) 16 juni 2015, nr. 64569/09 (*Delfi AS t. Estland*), ECLI:CE:ECHR:2015:0616JUD006456909, *EHRC* 2015/172 m.nt. B. van der Sloot, *NJB* 2015/1630, *NJ* 2016/457 m.nt. E.J. Dommering, par. 54 e.v.

408 Vgl. EHRM 20 september 2011 (ontv.), nr. 48703/08, ECLI:CE:ECHR:2011:0920DEC004870308 (*Verein gegen Tierfabriken t. Zwitserland*). Zie nader Gerards 2017d.

409 HvJ EU 27 maart 2014, zaak C-314/12, ECLI:EU:C:2014:192 (*UPC Telekabel Wien*), *EHRC* 2014/138 m.nt. C. Mak, par. 63.

410 De rechtspraak van het EHRM hierover beperkt zich tot toegang tot informatie die in handen is van de overheid; zie Gerards 2017c, C.1.2.

om een gedachte, geweten of godsdienst te hebben (het 'forum internum').[411] Daarop is in paragraaf II.1.3 al kort ingegaan. De godsdienstvrijheid beschermt echter ook de vrijheid om uitdrukking te geven aan een bepaalde religie (het 'forum externum').[412] Art. 6 Gw noemt in dit verband het recht om zijn godsdienst of levensovertuiging, individueel of in gemeenschap met anderen, vrij te belijden. Art. 9 lid 1 EVRM en art. 10 lid 1 10 Hv voegen hieraan nog toe dat het daarbij kan gaan om erediensten, onderricht, praktische toepassing of het onderhouden van geboden en voorschriften. Ook art. 18 IVBPR beschermt deze rechten.

Specifieke aspecten van de godsdienstvrijheid worden in Nederland en de EU via wetgeving en richtlijnen beschermd.[413] In het bijzonder biedt de Algemene wet gelijke behandeling (AWGB) – in lijn met de relevante Europese gelijkebehandelingsrichtlijnen – de nodige bescherming, vooral waar het gaat om directe of indirecte discriminatie vanwege bepaalde religieuze uitingen. In paragraaf II.2 is ingegaan op de werking van de AWGB. Daar is ook gebleken dat de godsdienstvrijheid via de AWGB een zekere horizontale werking toekomt, in die zin dat het ook voor private actoren zoals werkgevers en dienstverleners niet is toegestaan om mensen achter te stellen op basis van hun godsdienst.[414] Tegelijkertijd heeft het EHRM duidelijk gemaakt dat gewone burgers (anders dan bijvoorbeeld ambtenaren) geen verplichting hebben om neutraliteit uit te dragen.[415] Bovendien wordt de godsdienstvrijheid extra beschermd doordat bepaalde codificaties, zoals art. 2:2 Burgerlijk Wetboek en de AWGB, een bijzondere status geven aan religieuze instellingen en kerkge-

411 Zie o.m. Vermeulen & Van Roosmalen 2018; Van den Heede 2015, C.4; Vermeulen 2009; Schuyt 2008; Evans 2001.

412 Zie nader Vermeulen & Van Roosmalen 2018; Van den Heede 2015, C.5.

413 Voor de EU is bijvoorbeeld ook van belang dat asielzoekers op grond van art. 9 van de Terugkeerrichtlijn bescherming moeten krijgen wanneer zij het risico lopen in hun thuisstaat te worden vervolgd vanwege hun religie, ongeacht de vraag of dat is vanwege hun opvattingen of vanwege het geven van uitdrukking daaraan; zie o.m. HvJ EU 5 september 2012, gev. zaken C-71/11 en C-99/11, ECLI:EU:C:2012:518 (*Y en Z*), *EHRC* 2013/1 m.nt. B. Aarrass en K.M. de Vries en zie Nieuwenhuis 2013a, p. 57. Voor Nederland is daarnaast regelgeving relevant die weigering van bepaalde voorzieningen reguleert vanwege gewetensbezwaren, net als de Wet Openbare Manifestaties die godsdienstuitoefening buiten besloten plaatsen regelt; zie nader Nieuwenhuis 2013b, p. 59 en 62.

414 Ook dit is in lijn met de Europese richtlijnen, zoals ook blijkt uit de rechtspraak van het HvJ EU hierover; wel laat die zien dat in horizontale rechtsverhoudingen vaak meer vrijheid voor werkgevers en dienstverleners bestaat om beperkingen te stellen aan godsdienstige uitingen, ook al is de vraag of dat helemaal in lijn is met de rechtspraak van het EHRM; zie HvJ EU 14 maart 2017, zaak C-157/15, ECLI:EU:C:2017:203 (*Achbita*), *EHRC* 2017/96 m.nt. J.H. Gerards, *AB* 2017/162 m.nt. M.L.P. Loenen, *JAR* 2017/96 m.nt. E. Cremers-Hartman, *TRA* 2017/66 m.nt. N. Gundt en HvJ EU 14 maart 2017, zaak C-188/15, ECLI:EU:C:2017:204 (*Bougnaoui*), *EHRC* 2017/97 m.nt. J.H. Gerards onder *EHRC* 2017/96, *AB* 2017/163 m.nt. M.L.P. Loenen, *JAR* 2017/97 m.nt. E. Cremers-Hartman. Zie voor een voorbeeld van (indirecte) horizontale werking van de godsdienstvrijheid ook EHRM 15 januari 2013, nrs. 48420/10 e.a., ECLI:CE:ECHR:2013:0115JUD004842010 (*Eweida e.a. t. het Verenigd Koninkrijk*), *EHRC* 2013/67 m.nt. J.H. Gerards.

415 EHRM 5 december 2017, nr. 57792/15, ECLI:CE:ECHR:2017:1205JUD005779215 (*Hamidovic t. Bosnië-Herzegovina*), par. 40.

nootschappen. Zo sluit de AWGB kerkgenootschappen uit van de reikwijdte van het discriminatieverbod.[416] Daardoor kunnen binnen kerkgenootschappen gevallen van ongelijke behandeling worden toegelaten (zoals het uitsluiten van vrouwen van bepaalde functies of het niet willen aangaan van contractuele relaties), zonder dat het recht daaraan in de weg staat.[417] Ook een aantal organisatorische vereisten uit het Burgerlijk Wetboek vindt vanwege de bijzondere aard van de kerkgenootschappen geen toepassing.[418] Het vinden van een goede balans tussen de verschillende rechten en belangen is in de praktijk bijzonder complex, waardoor er geen handzame regels zijn aan te wijzen om aan te geven welke rechten of belangen in een concreet geval de voorrang zullen hebben.

Er bestaat veel discussie over de vraag welke aspecten van het forum externum precies worden beschermd. Dat heeft er allereerst mee te maken dat het moeilijk te bepalen is wat een godsdienst of levensovertuiging precies is.[419] Bij erkende godsdiensten als het katholicisme of de islam is dat nog wel duidelijk, maar lastiger wordt het bij controversiële religies als het pastafarisme of de Scientology Church.[420] Daarnaast geldt dat zelfs bij erkende godsdiensten, lang niet alle uitingen even breed gedeeld worden.[421] Zo is er discussie mogelijk over de vraag of het dragen van een hoofddoek voor vrouwen een religieus voorschrift is of niet. In de rechtspraak wordt dit meestal opgelost door af te gaan op een combinatie van objectieve en subjectieve criteria.[422] Een geloofsovertuiging moet een zekere mate van coherentie en serieusheid hebben, maar tegelijkertijd wordt al snel afgegaan op de stellingen van een gelovige over wat hij als een religieuze uiting ziet of niet.[423] Alleen als een handelen in een te ver verwijderd verband lijkt te staan van een godsdienst of levensovertuiging, of als het handelen voortkomt uit een zuiver individuele opvatting,

416 Art. 3 AWGB.

417 Zie nader Vermeulen 2006; Nieuwenhuis 2013b, p. 63-64.

418 Zie art. 2:2 BW.

419 Meestal wordt overigens niet echt onderscheid gemaakt tussen godsdienst, religie of levensovertuiging; deze begrippen kunnen voor het doel van deze paragraaf als synoniemen worden gezien; zie nader Van den Heede 2015, C.1.

420 Zie over het pastafarisme het oordeel van het College voor de Rechten van de Mens van 11 december 2017, oordeel 2017-145. Zie over Scientology onder meer EHRM 5 april 2007, nr. 18147/02, ECLI:CE:ECHR:2007:0405JUD001814702 (*Church of Scientology Moscow t. Rusland*). Voor een overzicht van godsdiensten en levensovertuigingen die het EHRM onder art. 9 EVRM heeft erkend, zie Van den Heede 2015, C.1; zie uitgebreid hierover ook Vermeulen & Van Roosmalen 2018.

421 Vgl. bijv. EHRM (GK) 26 april 2016, nr. 62649/10, ECLI:CE:ECHR:2016:0426JUD006264910 (*İzzettin Doğan e.a. t. Turkije*), *EHRC* 2016/167 m.nt. A.J. Overbeeke, par. 122.

422 Zie nader Vermeulen & Van Roosmalen 2018; Van den Heede 2015, C.5. Zie voor het EHRM onder meer EHRM 15 januari 2013, nrs. 48420/10 e.a., ECLI:CE:ECHR:2013:0115JUD004842010 (*Eweida e.a. t. het Verenigd Koninkrijk*), *EHRC* 2013/67 m.nt. J.H. Gerards, par. 80-81.

423 Idem. Zie recenter ook EHRM 6 april 2017, nrs. 10138/11 en 3 andere, ECLI:CE:ECHR:2017:0406JUD001013811 (*Klein e.a. t. Duitsland*), *EHRC* 2017/127 m.nt. M.R.T. Pauwels.

wordt het niet meer geaccepteerd als *religieuze* of levensbeschouwelijke uiting.[424] In dat geval kan overigens wel de vrijheid van meningsuiting nog van toepassing zijn.[425]

II.3.3.2 Beperkingen en verplichtingen

De godsdienstvrijheid is van groot belang voor de individuele ontplooiing in een pluralistische en diverse samenleving – in de woorden van het EHRM:

> 'This freedom is, in its religious dimension, one of the most vital elements that go to make up the identity of believers and their conception of life, but it is also a precious asset for atheists, agnostics, sceptics and the unconcerned. The pluralism indissociable from a democratic society, which has been dearly won over the centuries, depends on it.'[426]

De overheid heeft volgens vaste EHRM-rechtspraak dan ook tot belangrijke taak om het pluralisme in de democratische rechtsstaat actief te beschermen; dit is de 'collectieve dimensie' van de religieuze uitingsvrijheid.[427] Hieruit vloeien enkele belangrijke positieve verplichtingen voort, zoals een verplichting om gelovigen te beschermen tegen religieus gemotiveerde geweldpleging.[428] Daarnaast moet de overheid soms maatregelen treffen om ervoor te zorgen dat strijdende religieuze groepen elkaar tolereren.[429] Dit betekent overigens niet dat de staat zich zomaar mag mengen in de organisatie van geloofsgemeenschappen. Zo mag de staat zich niet bemoeien met de interne organisatie van geloofsgemeenschappen, bijvoorbeeld door te eisen dat binnen een geloofsrichting slechts een beperkt aantal geloofsgemeenschappen bestaat.[430] Evenmin mag de staat sturend optreden als zich interne kerkelijke conflicten voordoen.[431] Verder mag de staat zich niet uitspreken over de legiti-

---

424 Zie voor een aantal voorbeelden: Vermeulen & Van Roosmalen 2018; Van den Heede, C.5; Nieuwenhuis 2017b, p. 47.

425 Zie voor deze samenloop verder Nieuwenhuis 2017b, p. 50.

426 EHRM (GK) 1 juli 2014, nr. 43835/11, ECLI:CE:ECHR:2014:0701JUD004383511 (*S.A.S. t. Frankrijk*), *EHRC* 2014/208 m.nt. P.B.D.D.F. van Sasse van Ysselt, par. 124.

427 Vermeulen & Van Roosmalen 2018, p. 748 e.v.

428 Zie bijv. EHRM 7 oktober 2014, nr. 28490/02, ECLI:CE:ECHR:2014:1007JUD002849002 (*Begheluri e.a. t. Georgië*), *EHRC* 2015/10 m.nt. K. Henrard. Zie ook Vermeulen & Van Roosmalen 2018, p. 755; Van den Heede 2015, C.7; Nieuwenhuis 2013b, p. 56.

429 Bijv. EHRM (GK) 1 juli 2014, nr. 43835/11, ECLI:CE:ECHR:2014:0701JUD004383511 (*S.A.S. t. Frankrijk*), *EHRC* 2014/208 m.nt. P.B.C.D.F. van Sasse van Ysselt; zie ook Vermeulen & Van Roosmalen 2018, p. 751; Van den Heede 2015, C.7; Nieuwenhuis 2013b, p. 56.

430 Bijv. EHRM 23 maart 2017, nr. 40524/08, ECLI:CE:ECHR:2017:0323JUD004052408 (*Genov t. Bulgarije*), *EHRC* 2017/108. Zie nader Vermeulen & Van Roosmalen 2018, p. 751; Van den Heede 2015, C.8.1.

431 Bijv. EHRM 14 december 1999, nr. 38178/97, ECLI:CE:ECHR:1999:1214JUD003817897 (*Serif t. Griekenland*), *EHRC* 2000/14 m.nt. A.W. Heringa, AB 2000/73 m.nt. I. Sewandono, par. 51; Vermeulen & Van Roosmalen 2018, p. 751; Van den Heede 2015, C.8.1.

miteit van een bepaalde geloofsopvatting.[432] Wel is aanvaard dat de staat bepaalde eisen mag stellen als het gaat om het toebedelen van bijzondere voordelen aan kerkelijke of religieuze instellingen, zoals subsidies, belastingontheffingen of rechten om onderwijs te verzorgen.[433] De staat moet daarbij zeer zorgvuldig en neutraal te werk gaan, aan de hand van heldere en kenbare criteria.[434] Bovendien moet worden voorkomen dat de opvattingen en wensen van de meerderheid van de samenleving bovengeschikt worden gemaakt aan de opvattingen van (religieuze) minderheden of dat sprake is van misbruik van een dominante positie.[435]

Gaat het om individuele geloofsuitingen of -voorschriften als het dragen van hoofddoeken, kruisjes of schedelkapjes (al dan niet in openbare gebouwen), rituele slacht of het ophangen van crucifixen, dan laten de verschillende algemene grondrechtencodificaties nogal wat ruimte voor beperkingen.[436] Een rechtvaardiging voor dit soort beperkingen kan bijvoorbeeld worden gevonden in de wens tot scheiding van kerk en staat en het behouden van de neutraliteit van de openbare sfeer of in de wens tot het tegengaan van discriminatie op gronden als seksuele gerichtheid.[437] Een dergelijke rechtvaardiging moet niettemin overtuigend zijn en doel en middel moeten in een evenredige verhouding tot elkaar staan.[438] Voor Nederland geldt verder dat art. 6 Grondwet voor het toelaten van beperkingen onderscheid maakt tussen uitoefening van de godsdienstvrijheid binnen en buiten gesloten

---

432 EHRM (GK) 1 juli 2014, nr. 43835/11, ECLI:CE:ECHR:2014:0701JUD004383511 (*S.A.S. t. Frankrijk*), *EHRC* 2014/208 m.nt. P.B.C.D.F. van Sasse van Ysselt, par. 127.

433 Zie hierover de verschillende bijdragen in Broeksteeg & Terlouw 2011.

434 Met name het EHRM hecht sterk aan deze neutraliteit; zie nader Van den Heede 2015, C.2. en zie bijv. EHRM (GK) 26 april 2016, nr. 62649/10, ECLI:CE:ECHR:2016:0426JUD006264910 (*İzzettin Doğan e.a. t. Turkije*), *EHRC* 2016/167 m.nt. A.J. Overbeeke.

435 EHRM (GK) 1 juli 2014, nr. 43835/11, ECLI:CE:ECHR:2014:0701JUD004383511 (*S.A.S. t. Frankrijk*), *EHRC* 2014/208 m.nt. P.B.C.D.F. van Sasse van Ysselt, par. 128.

436 Zie resp. EHRM 5 december 2017, nr. 57792/15, ECLI:CE:ECHR:2017:1205JUD005779215 (*Hamidovic t. Bosnië-Herzegovina*), par. 38; EHRM (GK) 27 juni 2000, nr. 27417/95, ECLI:CE:ECHR:2000:0627JUD002741795 (*Cha'are Shalom ve Tsedek t. Frankrijk*), *EHRC* 2000/66 m.nt. J.H. Gerards, *AB* 2001/116 m.nt. B.P. Vermeulen, *NJCM-Bull.* 2001, p. 328 m.nt. C.D. de Jong; EHRM (GK) 18 maart 2011, nr. 30814/06, ECLI:CE:ECHR:2011:0318JUD003081406 (*Lautsi e.a. t. Italië*), *EHRC* 2010/8, *NJ* 2011/588 m.nt. E.A. Alkema, *NJCM-Bull.* 2010, p. 294 m.nt. A.C. Hendriks & A.B. Terlouw. Zie verder Vermeulen & Van Roosmalen 2018, p. 741; Nieuwenhuis 2013b, p. 54.

437 Zie bijv. EHRM (GK) 1 juli 2014, nr. 43835/11, ECLI:CE:ECHR:2014:0701JUD004383511 (*S.A.S. t. Frankrijk*), *EHRC* 2014/208 m.nt. P.B.C.D.F. van Sasse van Ysselt; EHRM 15 januari 2013, nrs. 48420/10 e.a., ECLI:CE:ECHR:2013:0115JUD004842010 (*Eweida e.a. t. het Verenigd Koninkrijk*), *EHRC* 2013/67 m.nt. J.H. Gerards.

438 Nader Van den Heede 2015, C.8; Nieuwenhuis 2013a, p. 53 e.v. Zie voor een voorbeeld waarin dit niet voldoende was aangetoond EHRM 5 december 2017, nr. 57792/15, ECLI:CE:ECHR:2017:1205JUD005779215 (*Hamidovic t. Bosnië-Herzegovina*). Zie over de te stellen eisen ook, met een andere invalshoek, HvJ EU 14 maart 2017, zaak C-157/15, ECLI:EU:C:2017:203 (*Achbita*), *EHRC* 2017/96 m.nt. J.H. Gerards, *AB* 2017/162 m.nt. M.L.P. Loenen, *JAR* 2017/96 m.nt. E. Cremers-Hartman, *TRA* 2017/66 m.nt. N. Gundt en HvJ EU 14 maart 2017, zaak C-188/15, ECLI:EU:C:2017:204 (*Bougnaoui*), *EHRC* 2017/97 m.nt. J.H. Gerards onder *EHRC* 2017/96, *AB* 2017/163 m.nt. M.L.P. Loenen, *JAR* 2017/97 m.nt. E. Cremers-Hartman.

plaatsen, waarbij clausuleringen binnen gesloten plaatsen (bijvoorbeeld religieuze gebouwen) alleen bij formele wet kunnen worden gesteld.[439]

II.3.4 Demonstratievrijheid

II.3.4.1 Codificaties en reikwijdte

De demonstratie- of betogingsvrijheid wordt gegarandeerd in art. 9 Gw, art. 11 EVRM, art. 12 Hv en art. 21 IVBPR. Art. 9 Gw is voor Nederland bovendien nader uitgewerkt in de Wet Openbare Manifestaties.[440] Het gaat daarbij steeds om *vreedzame* vergaderingen, protesten en bijeenkomsten – hebben de organisatoren van begin af aan al bedoeld om geweld te gebruiken, dan biedt de demonstratievrijheid geen bescherming.[441] Het is niet altijd gemakkelijk te bepalen of sprake is van een betoging of van een meningsuiting (of een uiting van een religieuze mening).[442,443] Meestal wordt de demonstratievrijheid gezien als een *specialis* ten opzichte van de hiervoor besproken vrijheden van meningsuiting en godsdienst.[444] Soms wordt als criterium gehanteerd dat bij een demonstratie sprake moet zijn van een samenkomst van twee of meer personen;[445] ontbreekt zo'n collectief element, dan gaat het om een meningsuiting.[446] Tegelijkertijd is aanvaard dat er ook eenpersoonsdemonstraties kunnen zijn (denk aan 'picketing': het zich met een banner of bord voor een gebouw posteren).[447] Demonstraties kunnen verder een uiteenlopend karakter hebben; het kan gaan om klassieke protestmarsen of samenkomsten op een plein, maar ook om blokkadeacties, sit-ins of demonstratieve kampementen.[448] Daarbij dekt de demonstratievrijheid niet alleen de vormkeuze, maar ook wensen van de organisatoren ten aanzien van de plaats en tijd waarop een demonstratie plaatsvindt.[449]

---

439 Nader Nieuwenhuis 2013b, p. 61.

440 Zie uitgebreid Roorda 2016, p. 30 e.v.

441 Nader Broeksteeg & Dorssemont 2017, C.2.1; Nieuwenhuis 2013c, p. 107. Zie bijv. EHRM 19 januari 2016, nr. 17526/10, ECLI:CE:ECHR:2016:0119JUD001752610 (*Gülcü t. Turkije*), *EHRC* 2016/77.

442 EHRM 20 juni 2017, nrs. 67667/09 en 2 andere, ECLI:CE:ECHR:2017:0620JUD006766709 (*Bayev e.a. t. Rusland*), *EHRC* 2017/158 m.nt. J.H. Gerards.

443 Zie Gerards 2017c, C.1.6; Roorda, p. 15 e.v.

444 Broeksteeg & Dorssemont 2017, C.1.; Nieuwenhuis 2013c, p. 110.

445 Bijv. EHRM 12 juni 2012, nrs. 26005/08 en 16160/08 (*Tátar en Fáber t. Hongarije*), ECLI:CE:ECHR:2012:0612JUD002600508, *EHRC* 2012/174, m.nt. J.H. Gerards.

446 Gerards 2017c, C.1.6.; Roorda 2016, p. 37 e.v.

447 Zie m.n. EHRM 7 februari 2017, nr. 57818/09 en 14 andere, ECLI:CE:ECHR:2017:0207JUD005781809 (*Lashmankin e.a. t. Rusland*), *EHRC* 2017/88 m.nt. B. Roorda, par. 363.

448 Broeksteeg & Dorssemont 2017, C.2.1.; Roorda 2016, p. 15 e.v.; Nieuwenhuis 2013c, p. 106.

449 Bijv. EHRM 7 februari 2017, nr. 57818/09 en 14 andere, ECLI:CE:ECHR:2017:0207JUD005781809 (*Lashmankin e.a. t. Rusland*), *EHRC* 2017/88 m.nt. B. Roorda, par. 405.

II.3.4.2 Beperkingen en verplichtingen

Beperkingen op de demonstratievrijheid kunnen redelijk zijn. Zo kan het nodig zijn om een demonstratie te beëindigen als die uit de hand dreigt te lopen of in geweld dreigt uit te monden, of om regulerend op te treden wanneer de openbare orde op bepaalde locaties in gevaar dreigt te worden gebracht. Gelet op het belang van de demonstratievrijheid in een democratische samenleving, mogen beperkingen echter niet te gemakkelijk worden opgelegd; demonstratieverboden zijn maar in heel uitzonderlijke gevallen toelaatbaar.[450] Uitgangspunt is juist dat de overheid verplicht is om ervoor te zorgen dat demonstraties zoveel mogelijk in de door de organisatoren gewenste vorm door kunnen gaan.[451] Daarbij rust op de staat onder meer een positieve verplichting om demonstranten zoveel mogelijk te beschermen wanneer tegendemonstranten hen proberen te hinderen.[452] Bovendien moeten goede voorbereidingsmaatregelen worden getroffen wanneer een demonstratie uit de hand dreigt te lopen om ervoor te zorgen dat de veiligheid van demonstranten zo goed mogelijk is verzekerd.[453]

Praktische beperkingen die vaak toelaatbaar zijn, zijn een kennisgevingsplicht of (voorafgaand opgelegde) beperkingen van plaats en tijd.[454] Dat soort beperkingen mag echter niet zodanig van aard zijn dat ze de demonstratie zijn nuttige functie ontnemen.[455] Het niet voldoen aan een kennisgevingsvereiste mag ook niet automatisch leiden tot een verbod op een demonstratie; daarvoor is alleen aanleiding wanneer er door het niet-tijdig aankondigen van een demonstratie grote problemen dreigen te ontstaan, bijvoorbeeld voor de openbare orde.[456] Beperkingen van vorm, tijd en plaats moeten bovendien redelijk en proportioneel zijn aan de doelen die ermee worden nagestreefd. Dat moet bij voorkeur per geval worden bekeken, zodat algemene verboden op demonstraties in de nabijheid

450 Nader Broeksteeg & Dorssemont 2017, C.2.2; Roorda 2016.

451 Bijv. EHRM 7 februari 2017, nr. 57818/09 en 14 andere, ECLI:CE:ECHR:2017:0207JUD005781809 (*Lashmankin e.a. t. Rusland*), *EHRC* 2017/88 m.nt. B. Roorda, par. 405. Ook dan zijn overigens wel beperkingen toegestaan als ze aan de eisen van redelijkheid en proportionaliteit voldoen; zie nader Nieuwenhuis 2013c, p. 114.

452 Zie klassiek EHRM 21 juni 1988, nr. 10126/82, ECLI:CE:ECHR:1988:0621JUD001012682 (*Plattform 'Ärzte für das Leben' t. Oostenrijk*); zie ook bijv. EHRM 29 juni 2006, nr. 76900/01, ECLI:CE:ECHR:2006:0629JUD007690001 (*Öllinger t. Oostenrijk*), *EHRC* 2006/107. Zie nader Roorda 2016, p. 100 e.v.

453 Bijv. EHRM 21 oktober 2010, nr. 4916/07, 25924/08 en 14599/09, ECLI:CE:ECHR:2010:1021JUD000491607 (*Alekseyev t. Rusland*), *EHRC* 2011/6, m.nt. J.P. Loof; EHRM 5 januari 2016, nr. 74568/12, ECLI:CE:ECHR:2016:0105JUD007456812 (*Frumkin t. Rusland*), *EHRC* 2016/90 m.nt. R. de Jong.

454 Uitgebreid, met veel verwijzingen naar de relevante EHRM- en HvJ EU-rechtspraak: Roorda 2016, hst. 3, 4 en 5; Broeksteeg & Dorssemont 2017, C.2.2.; Nieuwenhuis 2013a, p. 119.

455 Idem.

456 Bijv. EHRM 17 juli 2007, nr. 25691/04, ECLI:CE:ECHR:2007:0717JUD002569104 (*Bukta e.a. t. Hongarije*), *EHRC* 2007/11, m.nt. J.P. Loof, *NJ* 2007/631 m.nt. E.A. Alkema. Zie ook Broeksteeg & Dorssemont 2017, C.2.2.

van, bijvoorbeeld, rechtbanken of parlementsgebouwen niet zomaar zijn toegestaan.[457] Bovendien moet duidelijk zijn dat de doelstellingen legitiem zijn; beperkingen vanwege de inhoud van een demonstratie zijn niet toegestaan.[458]

II.3.5 Vrijheid van vereniging

II.3.5.1 Codificatie en reikwijdte

De vrijheid van vereniging is op diverse plaatsen in internationale verdragen gecodificeerd. Het recht is te vinden in art. 22 IVBPR, art. 11 EVRM en art. 12 Hv. Daarnaast is het recht opgenomen in art. 8 Gw. De codificatie in de Grondwet is zeer open geformuleerd – de bepaling stelt slechts dat het recht tot vereniging wordt erkend. De internationale bepalingen bevatten iets meer aanwijzingen met betrekking tot de reikwijdte van dit grondrecht. Zo vermelden de genoemde verdragsbepalingen allemaal dat de verenigingsvrijheid ook het recht omvat om vakverenigingen op te richten of zich daarbij aan te sluiten. De vakverenigingsvrijheid wordt – naast door de al genoemde bepalingen – ten slotte beschermd door tal van internationale verdragen op het terrein van de sociale grondrechten, zoals het ESH en ILO-verdragen. Art. 12 Hv specificeert bovendien dat de verenigingsvrijheid alle niveaus betreft, met name 'op politiek, vakverenigings- en maatschappelijk gebied'. Deze specificatie maakt duidelijk dat de verenigingsvrijheid ook een politiek karakter heeft, wat betekent dat politieke bewegingen en politie partijen er in het bijzonder door worden beschermd. Hoewel dit niet met zoveel woorden tot uitdrukking komt in de Grondwet of in de tekst van het EVRM, blijkt uit de rechtspraak over deze bepalingen dat de politieke verenigingsvrijheid een bijzondere betekenis toekomt.

Behalve in de Grondwet is in Nederland de verenigingsvrijheid op tal van andere plaatsen geregeld. Zo bevat het Burgerlijk Wetboek nadere bepalingen over de interne organisatievrijheid van verenigingen, de statuten en het lidmaatschap (zie art. 2:26 BW e.v.). Bovendien bevat het BW een bepaling over het ontbinden van verenigingen waarvan de werkzaamheden in strijd zijn met de openbare orde (art. 2:20 BW). Worden de werkzaamheden van een ontbonden vereniging toch voortgezet, dan is dit strafbaar op grond van art. 140 Sr.[459] Voor politieke partijen zijn er daarnaast nog allerlei specifieke regelingen die de politieke verenigingsvrijheid deels nader beschermen, maar deels ook beperkingen mogelijk maken. Het gaat dan in het bijzonder om eisen die worden gesteld als een vereni-

457 EHRM 7 februari 2017, nr. 57818/09 en 14 andere, ECLI:CE:ECHR:2017:0207JUD005781809 (*Lashmankin e.a. t. Rusland*), *EHRC* 2017/88 m.nt. B. Roorda; zie ook Broeksteeg & Dorssemont 2017, C.2.1.

458 Bijv. EHRM 21 oktober 2010, nr. 4916/07, 25924/08 en 14599/09, ECLI:CE:ECHR:2010:1021JUD000491607 (*Alekseyev t. Rusland*), *EHRC* 2011/6, m.nt. J.P. Loof.

459 Nieuwenhuis 2013c, p. 120.

ging als politieke partij wil deelnemen aan de verkiezingen, een onderwerp waarop hierna afzonderlijk in paragraaf II.3.6 zal worden ingegaan.

In algemene zin is de rechtspraak van het EHRM over de verenigingsvrijheid leidend voor de Nederlandse rechtspraktijk. In deze rechtspraak is een aantal hoofdpunten terug te vinden die betrekking hebben op de reikwijdte van de verenigingsvrijheid:[460]

- De verenigingsvrijheid heeft alleen betrekking op 'private' verenigingen. Zodra een vereniging een publiekrechtelijk karakter draagt, wat betekent dat de vereniging is ingebed in de structuren van de staat, is art. 11 EVRM niet van toepassing.[461] In het bijzonder betekent dit dat beroepsverenigingen die wettelijke taken uitoefenen, zoals regulering van het beroepsveld, uitvoering van tuchtrecht en educatie, niet kunnen worden gezien als verenigingen in de zin van art. 11 EVRM.
- De verenigingsvrijheid omvat een recht om zich te verenigen (oprichtingsvrijheid) of lid te worden van een vereniging (positieve verenigingsvrijheid), zonder dat dit nadelige consequenties heeft voor de betrokkenen.[462] Zo valt het ontslag van een ambtenaar wegens lidmaatschap van een bepaalde politieke partij binnen het bereik van de verenigingsvrijheid.[463]
- De verenigingsvrijheid beschermt het recht om niet gedwongen te worden lid te zijn van een vereniging (negatieve verenigingsvrijheid).[464] Belangrijk is tegelijkertijd dat ook de negatieve verenigingsvrijheid alleen geldt bij private verenigingen. De verplichting om lid te worden van een publieke vereniging – bijvoorbeeld om een bepaald beroep te kunnen uitoefenen – valt niet binnen het bereik van art. 11 EVRM en wordt dan ook niet verdragsrechtelijk beschermd.[465]
- De vakverenigingsvrijheid heeft een individuele dimensie, zoals het lid mogen worden (of juist niet lid hoeven te zijn) van een vakbond, of het niet lijden van nadeel (zoals

460 Zie nader ook Nieuwenhuis 2013c, p. 107-108.

461 Zie klassiek EHRM 23 juni 1981, nrs. 6878/75 en 7238/75, ECLI:CE:ECHR:1982:1018JUD000687875 (*Le Compte, Van Leuven en De Meyere t. België*) en EHRM 29 april 1999 (GK), nr. 25088/94 e.a., ECLI:CE:ECHR:1999:0429JUD002508894 (*Chassagnou t. Frankrijk*), *JB* 1999/186 m.nt. Heringa; zie recenter bijv. EHRM 20 januari 2011, nr. 9300/07, ECLI:CE:ECHR:2011:0120JUD000930007 (*Herrmann t. Duitsland*), *EHRC* 2011/52 m.nt. J.H. Gerards, bevestigd door de Grote Kamer op 26 juni 2012, *EHRC* 2012/176; EHRM 3 december 2015, nr. 29389/11, ECLI:CE:ECHR:2015:1203JUD002938911 (*Mytilinaios en Kostakis t. Griekenland*), *EHRC* 2016/56 m.nt. J.H. Gerards. Vgl. Broeksteeg & Dorssemont 2017, C.3.1; Nieuwenhuis 2013c, p. 107. Zie voor Nederland bijv. ABRvS 10 augustus 1999, *AB* 2000/168; ABRvS 9 januari 2008, *GJ* 2008/37 m.nt. Y.M. Drewes & A.C. Hendriks.

462 Nader Broeksteeg & Dorssemont 2017, C.3.2.

463 Zie klassiek EHRM 26 september 1995, nr. 17851/91, ECLI:CE:ECHR:1995:0926JUD001785191 (*Vogt t. Duitsland*). Zie verder Broeksteeg & Dorssemont 2017, C.3.4; Nieuwenhuis 2013c, p. 115.

464 Zie klassiek EHRM 23 juni 1981, nrs. 6878/75 en 7238/75, ECLI:CE:ECHR:1982:1018JUD000687875 (*Le Compte, Van Leuven en De Meyere t. België*) en EHRM 30 juni 1993 (*Sigurdur A. Sigurjónsson t. IJsland*), nr. 16130/90, ECLI:CE:ECHR:1993:0630JUD001613090. Zie verder Broeksteeg & Dorssemont 2017, C.3.3; Nieuwenhuis 2013c, p. 109; Gerards bij *EHRC* 2011/52 en *EHRC* 2016/56.

465 Zie de jurisprudentie hierboven genoemd.

ontslag) vanwege lidmaatschap van een vakbond.[466] Daarnaast is er een aantal connexe, collectieve rechten, zoals het recht om niet te worden uitgesloten van collectieve onderhandelingen en het recht op collectieve actie.[467]

In een enkel geval is het denkbaar dat een vereniging niet de bescherming geniet van art. 11 EVRM omdat de doelstellingen en handelingen ervan volledig in strijd zijn met de grondslagen waarop het EVRM rust. In dat geval wordt de bescherming van art. 11 EVRM weggenomen door art. 17 EVRM.[468]

De verenigingsvrijheid zoals neergelegd in de verdragen en in de Grondwet beschermt primair tegen de staat en niet zozeer tegen derden. Ook privépersonen kunnen echter inbreuk maken op de verenigingsvrijheid; zo kan het bestuur van een vereniging bijvoorbeeld mensen uitsluiten van het lidmaatschap of het lidmaatschap van iemand beëindigen. Gelet op het grondrechtelijk belang van de verenigingsvrijheid, is dit normaal gesproken iets waarmee de staat zich niet zal bemoeien. Niettemin gelden wel enkele bijzondere regels waar het gaat om botsing van de verenigingsvrijheid en andere grondrechten, zoals het non-discriminatierecht. Zo omvat art. 6a Algemene wet gelijke behandeling (AWGB) bijzondere regels over het lidmaatschap van vakverenigingen, die veel ruimte geven aan deze verenigingen om hun lidmaatschap en interne inrichting te bepalen.[469]

II.3.5.2 Beperkingen en verplichtingen

Net zoals voor de andere hiervoor beschreven vrijheden, geldt voor de vrijheid van vereniging dat redelijke beperkingen mogelijk zijn. Art. 6 Gw bepaalt bijvoorbeeld dat de verenigingsvrijheid bij de wet kan worden beperkt in het belang van de openbare orde. De specifieke bepalingen over statuten, lidmaatschap en ontbinding in Boek 2 BW zijn hiervan een

466 Bijv. EHRM 8 november 2016, nr. 26126/07, ECLI:CE:ECHR:2016:1108JUD002612607 (*Naku t. Litouwen en Zweden*), *EHRC* 2017/14. Zie over de individuele dimensie nader Broeksteeg & Dorssemont 2017, C.3.4.4.

467 Bijv. EHRM 4 april 2017, nr. 35009/05, ECLI:CE:ECHR:2017:0404JUD003500905 (*Tek Gıda İş Sendikası t. Turkije*), *JAR* 2017/153; EHRM 8 april 2014, nr. 31045/10, ECLI:CE:ECHR:2014:0408JUD003104510 (*The National Union of Rail, Maritime and Transport Workers t. het Verenigd Koninkrijk*), *EHRC* 2014/168 m.nt. F. Dorssemont; *JAR* 2014/128 m.nt. E. Koot-van der Putte. Zie nader Broeksteeg & Dorssemont 2017, C.3.4.4. Nieuwenhuis 2013c, p. 108.

468 Zie bijv. EHRM 12 juni 2012 (ontv.), nr. 31098/08, ECLI:CE:ECHR:2012:0612DEC003109808 (*Hizb Ut-Tahrir e.a. t. Duitsland*), *EHRC* 2012/201 m.nt. P.E. de Morree en EHRM 14 maart 2013, nrs. 26261/05 en 26377/06, ECLI:CE:ECHR:2013:0314JUD002626105 (*Kasymakhunov en Saybatalov t. Rusland*), *EHRC* 2013/122 m.nt. P.E. de Morree. Zie nader ook Broeksteeg & Dorssemont 2017, C.3.1; De Morree 2016; Nieuwenhuis 2013c, p. 112.

469 Zie nader Zoontjens 2006, p. 181 e.v. Ook het EVRM heeft tot op zekere hoogte indirecte horizontale werking in zaken over vakbondsvrijheid; zie bijv. de al genoemde zaak EHRM 8 november 2016, nr. 26126/07, ECLI:CE:ECHR:2016:1108JUD002612607 (*Naku t. Litouwen en Zweden*), *EHRC* 2017/14 en vgl. Nieuwenhuis 2013c, p. 118.

uitwerking. Ook art. 11 lid 2 EVRM en art. 52 lid 1 Hv bevatten mogelijkheden tot beperking van de verenigingsvrijheid.

Waar het gaat om de beperkingsmogelijkheden is voor de Nederlandse rechtspraktijk opnieuw de EHRM-rechtspraak leidend gebleken. Het EHRM heeft in zijn rechtspraak steeds vooropgesteld dat de verenigingsvrijheid van bijzonder belang is voor een goed functionerende democratische rechtsstaat.[470] Dat geldt in het bijzonder als het gaat om de politieke verenigingsvrijheid, die het EHRM sterk verbindt met het kiesrecht (zie hierna, paragraaf II.3.6) en de vrijheid van meningsuiting.[471] Dit betekent dat beperkingen in het algemeen niet gemakkelijk toelaatbaar zijn. Net als bij de andere vrijheidsrechten heeft ook bij de verenigingsvrijheid de staat bovendien een verplichting om actief beschermend op te treden, bijvoorbeeld om een vereniging te beschermen tegen geweld door tegenstanders.[472]

Als beperkingen worden gesteld aan het oprichten of registreren van politieke partijen of aan hun deelname aan het politieke leven, of als wordt besloten om een politieke partij te ontbinden, dan moeten daarvoor zeer zwaarwegende redenen bestaan.[473] Zo is een ontbinding van politieke partijen alleen aanvaardbaar wanneer de partij een direct risico oplevert voor het goed functioneren en voortbestaan van de democratische orde, blijkend uit concrete feiten en omstandigheden.[474] Ook de Nederlandse rechter heeft dergelijke strenge eisen gesteld, vooral bij politieke partijen, maar ook bij andere verenigingen.[475] Voor niet primair politieke verenigingen of bewegingen zijn de EHRM-eisen iets minder streng, maar ook daar moet steeds een legitiem doel worden gediend met een beperking en moet een verbod of beperking een proportionele maatregel zijn.[476] Datzelfde geldt bij vakverenigingen, zij het dat het EHRM daar een aanzienlijk ruimere beoordelingsvrijheid laat aan overheidsinstanties om te bekijken welke beperkingen eventueel mogen worden gesteld.

---

470 Bijv. EHRM (GK) 30 januari 1998, nr. 19392/92, ECLI:CE:ECHR:1998:0130JUD001939292 (*United Communist Party of Turkey e.a. t. Turkije*). Zie ook Broeksteeg & Dorssemont 2017, C.3.1; Nieuwenhuis 2013c, p. 108.

471 Nieuwenhuis 2013c, p. 108; De Morree 2016.

472 EHRM 20 oktober 2005, nr. 74989/01, ECLI:CE:ECHR:2005:1020JUD007498901 (*Ouranio Toxo e.a. t. Griekenland*), *EHRC* 2005/120.

473 Zie bijv. EHRM (GK) 17 februari 2004, nr. 44158/98, ECLI:CE:ECHR:2004:0217JUD004415898 (*Gorzelik e.a. t. Polen*), *EHRC* 2004/32 m.nt. H.L. Janssen, *NJ* 2005/420 n.nt. E.A. Alkema, *AB* 2002/180 m.nt. M.J. Kanne; zie ook Broeksteeg & Dorssemont 2017, C.3.2.1; Nieuwenhuis 2013c, p. 114 e.v.

474 Zie klassiek EHRM (GK) 13 februari 2003, nrs. 1340/98 e.a., ECLI:CE:ECHR:2003:0213JUD004134098 (*Refah Partisi e.a. t. Turkije*), *EHRC* 2003/28 m.nt. H.L. Janssen, *NJ* 2005/73 m.nt. E.A. Alkema, *AB* 2002/179 m.nt. M.J. Kanne. Zie nader Nieuwenhuis 2013c, p. 117.

475 Zie nader Nieuwenhuis 2013c, p. 120. Voor Nederland, zie bijv. Hoge Raad 18 april 2014, *NJ* 2014/507.

476 Zie bijv. EHRM 9 juli 2013, nr. 35943/10, ECLI:CE:ECHR:2013:0709JUD003594310 (*Vona t. Hongarije*), *EHRC* 2013/218 m.nt. P.E. de Morree, *NTM/NJCM-Bull.* 2014/41 m.nt. M.J. Kanne & J.L.W. Broeksteeg; EHRM 22 februari 2011, nr. 6468/09, ECLI:CE:ECHR:2011:0222DEC000646809 (*Association Nouvelle des Boulogne Boyst. Frankrijk*), *EHRC* 2011/93 m.nt. M.J. Kanne. Zie nader Broeksteeg & Dorssemont 2017, C.3.2.2.

II.3.6 Kiesrecht

Ten slotte is het kiesrecht van elementair belang in een democratische rechtsstaat. Het vormt een kernonderdeel van de politieke grondrechten. Het beoogt burgers voldoende invloed te laten hebben op de koers van het overheidsbeleid. Tussen het kiesrecht en de daaruit voortvloeiende meerderheid en de overige mensenrechtenbepalingen kan overigens een spanning ontstaan op het moment dat een meerderheidsbesluit op gespannen voet komt te staan met fundamentele rechten van minderheden. De rechtsstaat biedt dan als het goed is voldoende tegenwicht aan de democratisch gekozen meerderheid.

II.3.6.1 Codificaties en reikwijdte

Het kiesrecht is internationaal vastgelegd in diverse verdragen. De bepaling in het EVRM (art. 3 Eerste Protocol (EP)) is behoorlijk 'vaag' opgesteld in vergelijking met andere EVRM-bepalingen. Niettemin is de rechtspraak van het EHRM ondubbelzinnig en is het Hof van oordeel dat art. 3 EP afdwingbare (subjectieve) rechten vervat.[477] Art. 3 EP garandeert daardoor in de kern het recht om te stemmen (actief kiesrecht) en het recht om zichzelf kandidaat te stellen voor de wetgevende macht (passieve kiesrecht).[478] Bijzonder is ook dat een politieke partij de in art. 3 EP gewaarborgde rechten in kan roepen.[479] Het toepassingsbereik van art. 3 EP is beperkt tot verkiezingen van de 'wetgevende macht'. Slechts voor organen die daartoe behoren hebben verdragsstaten de verplichting vrije verkiezingen te organiseren overeenkomstig art. 3 EP. Dat hoeft overigens niet alleen te gaan om een wetgevende macht op centraal niveau; dat is afhankelijk van de constitutionele structuur van de betrokken staat.[480] Niettemin bestaat er in de literatuur discussie of de verkiezingen voor decentrale wetgevende organen binnen het bereik van art. 3 EP vallen.[481] Het orgaan moet wel wetgevende beslissingsbevoegdheid bezitten; een adviserende taak of een taak om alleen maar wetsvoorstellen in te dienen maakt niet dat een orgaan 'wetgevende macht' heeft. Het begrip 'effective political democracy' impliceert dat tevens wordt vereist dat het

477 EHRM 2 maart 1987, nr. 9267/81, ECLI:CE:ECHR:1987:0302JUD000926781 (*Mathieu-Mohin en Clerfayt t. België*), par. 48.

478 ECieRM 30 mei 1975, nrs. 6745/74 en 6746/74, ECLI:CE:ECHR:1975:0530DEC000674574 (*W, X, Y en Z t. België*); EHRM 2 maart 1987, nr. 9267/81, ECLI:CE:ECHR:1987:0302JUD000926781 (*Mathieu-Mohin en Clerfayt t. België*), par. 51.

479 EHRM 8 juli 2008, nr. 9103/04, ECLI:CE:ECHR:2008:0708JUD000910304 (*Georgische arbeiderspartij t. Georgië*), *EHRC* 2008/122 m.nt. J.L.W. Broeksteeg, par. 72.

480 EHRM 2 maart 1987, nr. 9267/81, ECLI:CE:ECHR:1987:0302JUD000926781 (*Mathieu-Mohin en Clerfayt t. België*), par. 53; EHRM 18 februari 1999, nr. 24833/94, ECLI:CE:ECHR:1999:0218JUD002483394 (*Matthews t. het Verenigd Koninkrijk*), *JB* 1999/64, *AB* 1999/181 m.nt. I. Sewandono, *NJ* 1999/515 m.nt. E.A. Alkema, par. 40.

481 Vgl. Barkhuysen & Van Emmerik 2013, p. 28.

orgaan instaat voor de democratische en politieke controle op het uitvoerend orgaan.[482] Als duidelijk is dat art. 3 EP van toepassing is, dan volgen uit deze bepaling en de interpretatie daarvan door het EVRM de volgende verplichtingen die onderling sterk met elkaar verbonden zijn:

- de verdragsstaten moeten vrije verkiezingen organiseren;
- de verkiezingen moeten met redelijke tussenpozen georganiseerd worden;
- de stemmen moeten geheim zijn;
- de verkiezingen moeten plaatsvinden onder zodanige condities dat de vrije meningsuiting van het volk bij het kiezen van de 'wetgevende macht' gewaarborgd is.

Op het niveau van de Europese Unie is het kiesrecht vastgelegd in art. 22 VWEU en art. 39 Hv. Art. 22 VWEU geeft iedere burger van de Unie die verblijf houdt in een lidstaat waarvan hij geen onderdaan is het actief en passief kiesrecht: bij de verkiezingen voor het Europees parlement en bij de gemeenteraadsverkiezingen in de lidstaat waar hij verblijft. Het kiesrecht wordt daarbij wel verleend onder dezelfde voorwaarden als aan de onderdanen van de lidstaat waar men verblijft. In twee richtlijnen zijn nadere regelingen getroffen door de Raad voor wat betreft beide verkiezingen.[483] In art. 39 Hv wordt het kiesrecht gewaarborgd van burgers van de Unie bij de verkiezingen van het Europees Parlement en in het tweede lid van deze bepaling worden de basisbeginselen van het kiesrecht in een democratisch bestel benadrukt. In art. 40 Hv ten slotte wordt dat gedaan voor het kiesrecht voor gemeenteraden voor personen die gebruik maken van het vrij verkeer en niet in zijn land van herkomst verblijft.

In art. 25 IVBPR is eveneens het actief en passief kiesrecht vastgelegd. In tegenstelling tot het EVRM blijft dat recht niet beperkt tot de wetgevende macht, maar betreft het een kiesrecht van vertegenwoordigers die deelnemen aan 'de behandeling van openbare aangelegenheden', tenminste voor zover er geen sprake is van rechtstreekse deelname van burgers en het bovendien expliciet als subjectief recht is geformuleerd voor elke burger.

Ten slotte is het kiesrecht vastgelegd in art. 4 Grondwet. Art. 4 Gw geldt voor alle Nederlanders. De reikwijdte van deze bepaling wordt bepaald door de term 'algemeen vertegenwoordigende organen'.[484] Daaronder vallen de Tweede Kamer, de Eerste Kamer alsmede Provinciale Staten en gemeenteraden, maar niet de besturen van de functioneel gedecen-

---

482 Goedertier & Haeck 2004, p. 463; zie voorts EHRM (GK) 22 december 2009, nrs. 27996/06 en 34836/06, ECLI:CE:ECHR:2009:1222JUD002799606 (*Sejdić en Finci t. Bosnië en Herzegovina*), *EHRC* 2010/17 m.nt. J.H. Gerards.

483 Richtlijn 94/80/EG voor gemeenteraadsverkiezingen en voor het kiesrecht bij de verkiezingen van het Europees parlement door middel van richtlijn 93/109/EG.

484 Van der Pot & Donner 2006, p. 330-331.

traliseerde overheidsorganisaties zoals de waterschappen. Bepalend is de aard en de omvang van de taken van een overheidsorganisatie. Art. 4 Gw kent een subjectief (individueel) grondrecht toe, politieke partijen worden beschermd door het hiervoor uiteengezette art. 8 Gw.

II.3.6.2 Beperkingen en verplichtingen

Voor wat betreft art. 3 EP mogen staten aan de uitoefening van dit recht voorwaarden verbinden waarbij tevens een ruime *margin of appreciation* door het Hof is toegekend.[485] Het EHRM toetst hierbij op drie elementen:

1. de nationale voorwaarden mogen de betrokken rechten niet in zo hoge mate beperken dat de rechten in hun kern worden aangetast;
2. de verdragsstaten moeten met de nationale voorwaarden een legitiem doel nastreven;
3. de aangewende middelen mogen niet disproportioneel zijn ten opzichte van het nagestreefde doel.

Belangrijk criterium hierbij is of er al dan niet sprake is van een verstoring van de vrije meningsuiting van het volk ten aanzien van de keuze van de wetgever.[486] Van belang is overigens dat art. 3 EP geen bepaald soort kiesstelsel oplegt. Het hanteren van een bepaalde kiesdrempel (onder omstandigheden bijv. 7%) is zelfs nog toelaatbaar volgens het EHRM.[487] Een aantal zaken heeft betrekking gehad op de vraag of een strafrechtelijke veroordeling aanleiding kan zijn om burgers het kiesrecht te ontnemen.[488]

---

485 EHRM 2 maart 1987, nr. 9267/81, ECLI:CE:ECHR:1987:0302JUD000926781 (*Mathieu-Mohin en Clerfayt t. België*), par. 52.

486 EHRM 9 april 2002, nr. 46726/99, ECLI:CE:ECHR:2002:0409JUD004672699 (*Podkolzina t. Letland*), *EHRC* 2002/41 m.nt. A.W. Heringa, par. 33; EHRM 2 maart 1987, nr. 9267/81, ECLI:CE:ECHR:1987:0302JUD000926781 (*Mathieu-Mohin en Clerfayt t. België*), par. 54 ; EHRM (GK) 8 juli 2008, nr. 10226/03, ECLI:CE:ECHR:2008:0708JUD001022603, *EHRC* 2007/110 m.nt. J.L.W. Broeksteeg (*Yumak en Sadak t. Turkije*), *EHRC* 2007/110 m.nt. J.L.W. Broeksteeg, par. 111 ; EHRM (GK) 6 maart 2003, nr. 58278/00, ECLI:CE:ECHR:2006:0316JUD005827800 (*Žd anoka t. Letland*), *EHRC* 2004/76.

487 Meest belangrijk is EHRM (GK) 8 juli 2008, nr. 10226/03, ECLI:CE:ECHR:2008:0708JUD001022603, *EHRC* 2007/110 m.nt. J.L.W. Broeksteeg (*Yumak en Sadak t. Turkije*), *EHRC* 2007/110 m.nt. J.L.W. Broeksteeg. Zie voor andere voorbeelden EHRM 7 juni 2001 (ontv.), nr. 56618/00, ECLI:CE:ECHR:2001:0607DEC005661800 (*Federacion Nacionalista Canaria t. Spanje*) (kiesdrempel van 6% expliciet goedgekeurd); EHRM 2 juli 2002 (ontv.), nr. 53180/99, ECLI:CE:ECHR:2002:0702DEC005318099 (*Gorizdra t. Moldavië*) (kiesdrempel van 4% expliciet goedgekeurd en redengeving); EHRM 8 juli 2008, nr. 9103/04, ECLI:CE:ECHR:2008:0708JUD000910304 (*Georgische arbeiderspartij t. Georgië*), *EHRC* 2008/122 m.nt. J.L.W. Broeksteeg (kiesdrempel van 7% impliciet goedgekeurd); EHRM 10 mei 2012, nr. 7819/03, ECLI:CE:ECHR:2012:0510JUD000781903 (*Özgürlük Ve Dayanisma Partisi (ÖDP) t. Turkije*), *EHRC* 2012/144 m.nt. J.L.W. Broeksteeg.

488 EHRM (GK) 6 oktober 2005, nr. 74025/01, ECLI:CE:ECHR:2005:1006JUD007402501 (*Hirst t. het Verenigd Koninkrijk*), *EHRC* 2005/115 m.nt. J.L.W. Broeksteeg, *NTM-NJCM-bull.* 2006, p. 234 m.nt. H. Sackers, par. 82; bevestigd in o.m. EHRM 23 november 2010, nrs. 60041/08 en 60054/08, ECLI:CE:ECHR:2010:1123JUD006004108 (*Greens e.a. t. het Verenigd Koninkrijk*), *EHRC* 2011/20, m.nt. R. de Lange, *NJ* 2012/285 m.nt. E.A. Alkema, *AB* 2011/123 m.nt. J. Uzman; EHRM 12 mei 2012, nr. 126/05,

Art. 25 IVBPR is, zoals hiervoor uiteengezet, ruim geredigeerd, daar staat tegenover dat het artikel beperkingen op het kiesrecht in ruimte mate toelaat, zolang deze beperkingen niet onredelijk zijn.[489] Tijdelijke ontneming van het kiesrecht van (onherroepelijk veroordeelde) gedetineerden met meer dan één jaar gevangenisstraf is bijvoorbeeld niet onredelijk.

Art. 4 Gw attribueert de bevoegdheid aan de wetgever om 'bij wet' beperkingen dan wel uitzonderingen te maken op het actief en passief kiesrecht. In de art. 54 en 56 Gw zijn voorts grondwettelijke vereisten gesteld aan het kiesrecht zoals het feit dat iemand ouder moet zijn dan 18 jaar of ouder moet zijn en niet moet zijn uitgesloten van het kiesrecht.

II.4 Procedurele rechten

II.4.1 Inleiding

Het recht op een effectief rechtsmiddel en op een eerlijk proces is een wezenlijk recht in een democratische rechtsstaat. Het zorgt voor rust in de samenleving als conflicten en overtredingen via een helder, objectief, neutraal en niet betrokken instituut kunnen worden beslecht, in plaats van via eigenrichting. Een andere belangrijke waarde van het hebben van een effectieve rechterlijke macht is dat die controle kan uitoefenen op het handelen van zowel niet-statelijke als statelijke actoren.[490] Andere (al dan niet fundamentele) rechten kunnen daardoor effectief worden verzekerd.[491] Als immers, bijvoorbeeld, iemand is aangetast in zijn vrijheid van meningsuiting of zijn eigendomsrechten, of als iemand is gediscrimineerd, is er een instrumentarium voorhanden waardoor de betrokkene zijn recht kan halen. Daarbij betekent het recht op een effectief rechtsmiddel dat zo'n instrumentarium ook daadwerkelijk wordt geboden, hetzij in de vorm van toegang tot een rechter (bijvoorbeeld een civiele of strafrechter), hetzij in een alternatieve vorm (bijvoorbeeld mediation). Wordt voorzien in zo'n rechtsmiddel, dan moet ervoor worden gezorgd dat de procedure eerlijk verloopt.

Natuurlijk roepen deze grove definities veel vragen op. Een eerste vraag is uiteraard wat het betekent dat een rechtsmiddel 'effectief' moet zijn en wanneer precies toegang tot zo'n rechtsmiddel moet worden geboden. Een tweede vraag is wat het betekent om te spreken van een 'eerlijk' proces. Antwoorden op deze vragen zijn in literatuur en rechtspraak met grote mate van verfijning gegeven. Tal van facetten van de beide rechten zijn bovendien gecodificeerd, vooral in internationale verdragen en in de toekomst mogelijk ook in de

---

ECLI:CE:ECHR:2012:0522JUD000012605 (*Scoppola t. Italië nr. 3*), *EHRC* 2012/154 m.nt. R. de Lange, *NJ* 2013/373 m.nt. B.E.P. Myjer.

489 Vgl. Barkhuysen & Van Emmerik 2013, p. 38.

490 Vgl. Bauw 2017, p. 17 e.v.; Bovend'Eert 2013, p. 13.

491 Idem.

Nederlandse Grondwet. Het is onmogelijk om in dit hoofdstuk een volledig overzicht te geven van alle rechten die samenhangen met het recht op een effectief rechtsmiddel en een eerlijk proces. Gelet op de vraagstelling van dit onderzoek is het ook niet nodig om dat te doen. Wel wordt in het navolgende een globaal overzicht gegeven van de meest belangrijke aspecten in verband met algoritme-gedreven besluitvorming: de toegang tot een effectief rechtsmiddel als zodanig; het recht op equality of arms; het recht op een onafhankelijke en onpartijdige rechter; het recht op een transparante en draagkrachtige motivering; en de presumptie van onschuld (specifiek voor het strafproces).

II.4.2 Het recht op een effectief rechtsmiddel

Zoals hiervoor al omschreven, is het voor het verwezenlijken van individuele rechten in een democratische rechtsstaat essentieel dat effectieve toegang tot het recht bestaat. Dit recht is voor het verwezenlijken van de EVRM-rechten specifiek verankerd in art. 13 EVRM.[492] Voor zover het gaat om kwesties die binnen het bereik van het EU-recht vallen, is het te vinden in art. 47 Hv.[493] Het recht op een effectief rechtsmiddel hangt nauw samen met het recht op toegang tot de rechter. Het belangrijkste verschil tussen de twee is dat een effectief rechtsmiddel niet noodzakelijkerwijze een 'rechter' hoeft te zijn – het kan bijvoorbeeld ook gaan om een bindende vorm van mediation of om een ad hoc ingesteld orgaan dat bindende beslissingen kan nemen. In veruit de meeste gevallen zijn rechtsbeschermingsmechanismen echter wel degelijk ingebed in de rechterlijke macht en moet de gang tot de rechter voor betrokkenen voldoende openstaan. Het Europees Hof voor de Rechten van de Mens heeft een dergelijk recht op toegang tot de rechter ingelezen in het recht op een eerlijk proces voor een onafhankelijke en onpartijdige rechter, neergelegd in art. 6 EVRM. De toegang tot de rechter ligt in het EU-Grondrechtenhandvest voor aan het EU-recht gerelateerde geschillen vast in art. 47, eerste zin, Hv. In de VN-mensenrechtenverdragen is het recht op toegang tot de rechter te vinden in art. 14 IVBPR. In de Nederlandse Grondwet is een expliciet recht op toegang tot de rechter momenteel niet te vinden. Gerelateerde rechten zijn wel gecodificeerd, zoals het recht om niet te worden afgehouden van de rechter die iemand toekomt (het *ius de non evocandi*). Om te voorzien in het gemis van een expliciete en heldere Grondwetsbepaling over het recht op toegang

492 Art. 13 EVRM: 'Een ieder wiens rechten en vrijheden die in dit Verdrag zijn vermeld, zijn geschonden, heeft recht op een daadwerkelijk rechtsmiddel voor een nationale instantie, ook indien deze schending is begaan door personen in de uitoefening van hun ambtelijke functie.'

493 Art. 47, eerste zin, Hv: 'Eenieder wiens door het recht van de Unie gewaarborgde rechten en vrijheden zijn geschonden, heeft recht op een doeltreffende voorziening in rechte, met inachtneming van de in dit artikel gestelde voorwaarden.'

tot de rechter, ligt momenteel wel een grondwetswijzigingsvoorstel voor dat is geaccepteerd door de Tweede Kamer.[494]

Naast deze algemene codificaties van procedurele en rechtsbeschermingsrechten, zijn er veel specifieke bepalingen waaruit in de loop van de tijd procedurele verplichtingen voor de staat en daarmee corresponderende individuele rechten zijn afgeleid. In het bijzonder het EHRM heeft uit tal van materiële grondrechtenbepalingen procedurele rechten afgeleid, ook waar het niet zozeer gaat om de eigenlijke rechterlijke procedure, maar eerder om de voorprocedure. Zo heeft het belangrijke eisen in het EVRM ingelezen waar het gaat om transparantie van besluitvormingsprocessen die leiden tot ingrijpende besluiten, waar het gaat om betrokkenheid van burgers bij de besluitvorming en waar het gaat om onderzoek en toegang tot de rechter als mensenrechtenschendingen zich hebben voorgedaan.[495]

De verschillende codificaties van het recht op een effectief rechtsmiddel en het recht op toegang tot de rechter verschillen in het bijzonder waar het gaat om hun toepassingsbereik. Het recht op een effectief rechtsmiddel van art. 13 EVRM bestaat volgens vaste rechtspraak van het EHRM alleen wanneer iemand zo'n rechtsmiddel wil gebruiken om bescherming van zijn EVRM-rechten te claimen. Daarvoor is het nodig dat er een 'arguable claim' kan worden gemaakt dat zo'n EVRM-recht aan de orde is.[496] Heeft een geschil betrekking op andere rechten of belangen dan door het EVRM worden beschermd, dan kan art. 13 EVRM geen rechtsbescherming bieden.

Art. 6 EVRM kent deze beperking niet, maar kent het recht op toegang tot de rechter toe als er (a) een daadwerkelijk geschil bestaat over de vaststelling van iemands burgerlijke rechten of verplichtingen of (b) wanneer sprake is van een strafvervolging.[497] De tekst letterlijk nemend zou dit betekenen dat veel bestuursrechtelijke geschillen buiten het bereik van art. 6 EVRM vallen. Het EHRM heeft in de loop van de tijd de (a)-grond echter zeer ruim geïnterpreteerd, waardoor tegenwoordig eigenlijk alleen nog die geschillen buiten het recht op toegang tot de rechter vallen die overduidelijk publiekrechtelijk van aard zijn en nauw zijn verbonden aan de prerogatieven van de staat – denk aan belastinggeschillen, geschillen over vreemdelingenrechtelijke vraagstukken, verkiezingskwesties of bepaalde

494 Kamerstuknr. 34517; beoogd wordt daaraan een nieuw artikellid toe te voegen met de tekst: 'Ieder heeft bij het vaststellen van zijn rechten en verplichtingen of bij het bepalen van de gegrondheid van een tegen hem ingestelde vervolging recht op een eerlijk proces binnen een redelijke termijn voor een onafhankelijke en onpartijdige rechter'.

495 Zie voor een recent en zeer volledig overzicht van deze verplichtingen De Jong 2017 en zie Reiertsen 2017, p. 390.

496 Zie uitgebreid Reiertsen 2017, p. 183 e.v.; zie korter ook De Jong 2017, p. 40 e.v.

497 Hetzelfde geldt voor art. 14 IVBPR. Zie voor de klassieke definitie van 'strafvervolging' EHRM 8 juni 1976, nrs. 5100/71 e.a., ECLI:CE:ECHR:1976:1123JUD000510071 (*Engel e.a. t. Nederland*), *NJ* 1978/223, *AB* 1978/223 m.nt. J. in 't Veld. Voor korte en heldere overzichten, zie De Jong 2017, p. 19-20; voor een meer uitgebreide analyse, zie het *Sdu Commentaar EVRM* (online via opmaat.sdu.nl), bijgewerkt tot en met 2017.

ambtenarenzaken.[498] Het toepassingsbereik is hierdoor zeer ruim geworden, al zijn er nog altijd kwesties waarop art. 6 EVRM niet van toepassing is. Art. 13 EVRM biedt hiervoor tot op zekere hoogte wel een vangnet: voor zover het gaat om kwesties die mensenrechtelijke aspecten hebben moet immers in ieder geval toegang bestaat tot een effectief rechtsmiddel, dat volgens de rechtspraak van het EHRM een groot aantal waarborgen moet bieden die ook een rechterlijke procedure biedt.[499] Ook art. 47 Hv heeft in zekere zin een beperkt toepassingsbereik, omdat het zich slechts uitstrekt tot 'door het recht van de Unie gewaarborgde rechten en vrijheden'. Bovendien leert art. 51 Hv dat het EU-Grondrechtenhandvest alleen van toepassing is in kwesties die vallen binnen het bereik van het EU-recht. Bij puur nationale geschillen, waarop ook geen implementatiewetgeving van toepassing is, kan art. 47 Hv dus niet worden ingeroepen. Het voorgestelde art. 17 lid 1 Grondwet voorziet in deze hiaten door te bepalen dat een recht op toegang tot een rechter bestaat 'bij het vaststellen van zijn rechten en verplichtingen of bij het bepalen van de gegrondheid van een tegen hem ingestelde vervolging'. Deze bepaling is echter nog geen geldend recht. Vooralsnog betekent dit dat zich gevallen kunnen voordoen, vooral in het publiekrecht, waarin de Europese grondrechtencodificaties niet voorzien in een recht op toegang tot de rechter of een effectief rechtsmiddel.

De rechten op effectieve rechtsbescherming, een effectief rechtsmiddel en de toegang tot een rechter, samen met de procedurele positieve verplichtingen die het EHRM heeft afgeleid uit de verschillende materiële EVRM-bepalingen, omvatten een groot aantal verschillende deelaspecten.

Allereerst is er een aantal verplichtingen voor de staat wanneer de staat verantwoordelijk is voor een dreigende aantasting van door het EVRM beschermde grondrechten. Het gaat daarbij om zeer uiteenlopende kwesties: besluitvorming over voor mensen en goederen gevaarlijke processen als gaswinning of de plaatsing van nieuwe fabrieken, preventie van ernstige ongevallen, evacuaties bij natuurrampen, voorlopige vrijlating van TBS'ers, uithuisplaatsing van kinderen, uitzetting van vreemdelingen, eigendomsontneming, tegengaan van huiselijk geweld, enzovoort. Hoewel de rechtspraak hierover heel verfijnd is, kan in algemeen worden gesteld dat er een aantal kernverplichtingen is voor de bevoegde autoriteiten:

– *Transparantie en informatievoorziening* – mensen voor wie besluiten grote gevolgen kunnen hebben, hebben het recht om informatie te verkrijgen over de (niet) te nemen besluiten en de eventuele gevolgen ervan.[500]

498 Zie kort, met verwijzingen naar relevante rechtspraak, De Jong 2017, p. 24-25.

499 Zie voor een nadere analyse van deze waarborgen in relatie tot die onder art. 6 EVRM: Reiertsen 2017, p. 232 e.v.

500 Sanderink 2015, hst. 8; De Jong 2017, bijv. p. 55, 160, 166 e.v.

- *Participatie* – betrokkenen moeten zo goed als mogelijk in de gelegenheid worden gesteld om effectief aan de besluitvorming deel te nemen, in ieder geval door hen te horen.[501]
- *Zorgvuldigheid* – de bevoegde autoriteiten moeten de verschillende bij ingrijpende besluiten betrokken belangen en feiten zo zorgvuldig en volledig mogelijk verzamelen en onderzoeken en moeten op basis van alle omstandigheden een degelijke, redelijke en niet-willekeurige belangenafweging maken.[502]
- *Regelgeving, toezicht en handhaving* – ter voorkoming van grondrechtenschendingen (door de staat zelf, maar ook door derden) moet de staat niet alleen voorzien in adequate regelstelsels, maar moet de staat ook toezicht houden op de naleving van die regels en waar nodig optreden waar ze (dreigen te) worden overtreden.[503]

Is eenmaal een ingrijpend besluit genomen waardoor EVRM-rechten zijn aangetast of is het effect van overheidsoptreden of nalaten dat individuele rechten en belangen zijn geschonden, dan moet de staat gedegen, snel en adequaat *onderzoek* verrichten dat er effectief toe kan leiden dat de verantwoordelijken worden opgespoord en – waar opportuun – worden berecht.[504]

Het sluitstuk van het recht op effectieve rechtsbescherming en een effectief rechtsmiddel is dat er in ieder geval een procedure beschikbaar is die kan leiden tot rechtsherstel. Onder art. 13 EVRM heeft het EHRM een uitgebreide jurisprudentie ontwikkeld waaruit blijkt wanneer sprake is van een *effectief* rechtsmiddel. Heel kort kan die als volgt worden samengevat:

- *Toegankelijkheid* – de rechtszoekende moet zelf zonder al te veel moeite het rechtsmiddel kunnen benaderen; het is bijvoorbeeld niet voldoende dat een institutie discretionaire vrijheid heeft om bepaalde kwesties te onderzoeken en dan rechtsherstel te bieden.[505]
- *Procedurele waarborgen* – zeker wanneer het gaat om een ander instituut dan een rechter moet ervoor worden gezorgd dat een eerlijke en goede procedure is ingericht.[506] De procedurele waarborgen onder art. 13 zijn in algemene zin iets minder verstrekkend dan die bij art. 6 EVRM, maar het EHRM heeft wel degelijk eisen gesteld aan onafhankelijkheid en onpartijdigheid, aan de toegang tot bewijs, aan de procedurele openheid

501 De Jong 2017, bijv. p. 152 (familierechtelijke kwesties), 160 (milieukwesties), 240 (eigendomsinmenging).
502 Sanderink 2015, hst. 5; De Jong 2017, bijv. p. 154-155 (familierechtelijke kwesties), 162 (milieukwesties), 241 (eigendomsinmenging).
503 Sanderink 2015, hst. 3, 4, 6 en 7; De Jong 2017, bijv. p. 52 e.v. (artikel 2 EVRM), p. 96 e.v. (artikel 3 EVRM), p. 148 e.v. (artikel 8 EVRM).
504 De Jong 2017, p. 61 e.v. (artikel 2 EVRM), p. 100 e.v. (artikel 3 EVRM), p. 150 e.v. (artikel 8 EVRM); Gerards, Barkhuysen & Van Emmerik 2014, p. 44-47.
505 Reiertsen 2017, p. 213 e.v.; De Jong 2017, p. 42.
506 Reiertsen 2017, p. 232 e.v.

en aan de gelijkheid van de partijen.[507] Op de verschillende eisen van een eerlijk proces wordt in paragraaf II.4.3 nog afzonderlijk ingegaan.
- *Rechtsherstel* – het rechtsmiddel moet kunnen leiden tot effectief rechtsherstel, inclusief een bindende uitspraak waarmee bijvoorbeeld een einde kan worden gemaakt aan een onrechtmatige situatie of schadevergoeding wordt geboden.[508] Rechtsmiddelen die niet tot bindende uitspraken kunnen leiden, zoals toegang tot een Ombudsman of in Nederland tot het College van de Mens, kunnen daardoor niet als effectief rechtsmiddel worden gezien in de zin van art. 13 EVRM.
- *Inhoudelijke beoordeling* – het rechtsmiddel moet het mogelijk maken een kwestie ten gronde te beoordelen.[509] Tegelijkertijd is het niet nodig dat wordt voorzien in bepaalde bijzondere rechtsmiddelen, zoals een mogelijkheid van constitutionele toetsing van wetgeving.
- *Snelheid* – effectief rechtsherstel moet met de nodige snelheid kunnen worden geboden.[510]

Soortgelijke vereisten zijn terug te vinden in de rechtspraak van het HvJ EU, waarbij dit Hof bovendien steeds benadrukt dat de rechtsmiddelen die voor het EU-recht beschikbaar zijn doeltreffend moeten zijn en gelijkwaardig aan die voor het nationale recht.[511]

De waarborgen van het recht op een effectief rechtsmiddel overlappen deels met de waarborgen die moeten worden geboden als onderdeel van het recht op toegang tot de rechter zoals dat door art. 6 EVRM en art. 47 Hv wordt beschermd. Gesteld kan worden dat de hiervoor genoemde vijf waarborgen ook van deze twee bepalingen de kern vormen. Aanvullend hierop garanderen art. 6 EVRM en art. 47 Hv in de interpretatie van het EHRM en het HvJ EU de volgende deelrechten:[512]
- *Onafhankelijkheid* – de rechter hoort onafhankelijk te zijn van andere statelijke actoren (zoals de uitvoerende macht) en van procespartijen.[513] Deze onafhankelijkheid kent verschillende aspecten:

507 Idem.
508 Reiertsen 2017, p. 248 e.v.
509 Reiertsen 2017, p. 250 e.v.
510 Reiertsen 2017, p. 299 e.v.
511 Zie bijv. Ward e.a. 2014, par. 47.57.
512 De interpretaties voor beide artikelen lopen grotendeels parallel, omdat het gaat om corresponderende bepalingen als bedoeld in art. 52 lid 3 Hv; wel kan het zijn dat het HvJ EU soms meer bescherming biedt dan het EHRM dat doet, maar echt groot zijn de verschillen vooralsnog niet. Wel heeft het HvJ EU besloten om stelselmatig alleen naar art. 47 Hv te verwijzen en niet meer naar art. 6 EVRM; zie nader Greer, Gerards & Slowe 2018, p. 360.
513 Bovend'Eert 2013, hst. 2; Van den Eijnden 2013; De Jong 2017, p. 29; Greer, Gerards & Slowe 2018, . Dit aspect komt ook in de Grondwet tot uitdrukking; zie art. 117. Veel van regels zijn voor Nederland uitgewerkt in de Wet rechtspositie rechterlijke ambtenaren.

- Persoonlijke onafhankelijkheid – er moeten voldoende waarborgen worden geboden rondom benoeming, ambtsduur en ontslag, zodat andere staatsmachten niet al te veel invloed kunnen hebben op het soort rechter dat wordt benoemd en geen druk kunnen uitoefenen op rechters om op een bepaalde manier te beslissen.[514]
- Zakelijke of functionele onafhankelijkheid – er moeten voldoende garanties zijn tegen druk van buitenaf om zaken op een bepaalde manier te beslechten en de rechter moet zelfstandig, zonder inmenging van de andere staatsmachten, tot zijn beslissing kunnen komen.[515]
- Institutionele onafhankelijkheid – de overheidsorganisatie waarvan rechters deel uitmaken moet een onafhankelijke positie kunnen innemen ten aanzien van de andere staatsmachten, bijvoorbeeld als het gaat om financiering, organisatie en werkwijze.[516]
- *Onpartijdigheid* – de rechter hoort onpartijdig te zijn, wat vooral betekent dat hij niet vooringenomen is ten opzichte van de zaak of ten opzichte van (een van) de partijen.[517] Vooral in de EHRM-rechtspraak worden hierbij twee aspecten onderscheiden:
- Subjectieve onpartijdigheid – de rechter mag geen zodanige verbondenheid hebben met de zaak of met (een van) de beide partijen die maakt dat hij niet meer objectief over de zaak kan oordelen; het gaat hier dus om zijn persoonlijke instelling en overtuiging.[518]
- Objectieve onpartijdigheid – de procedure moet zo zijn ingericht dat er geen legitieme twijfel mogelijk is over de objectiviteit van de rechter (of een rechterlijk college) bij de beoordeling van een zaak, onder het motto 'justice must not only be done, it must also seen to be done'.[519]

De rechtspraak over deze twee aspecten is sterk casuïstisch van aard, maar het element van ontbrekende 'bias' – hetzij subjectief, hetzij in de ogen van de buitenstaander – komt steeds weer terug.

- *Toegankelijkheid* – onnodige of disproportioneel hoge drempels die een rechtszoekende afhouden van effectieve toegang tot een rechterlijke procedure zijn niet aanvaardbaar:
- Al te hoge griffierechten of leges kunnen het recht op toegang tot de rechter disproportioneel aantasten.[520]
- Het ontbreken van door de staat gefinancierde rechtsbijstand kan in bepaalde gevallen in de weg staan aan het effectief kunnen voeren van een procedure.[521]

514 Bovend'Eert 2013, p. 18 e.v.
515 Bovend'Eert 2013, p. 21 e.v.
516 Bovend'Eert 2013, p. 27 e.v.
517 Bovend'Eert 2013, hst. 3.
518 Bovend'Eert 2013, p. 37 e.v.
519 Bovend'Eert 2013, p. 41 e.v.
520 Greer, Gerards & Slowe 2018, p. 362.
521 Zie uitgebreid Commissie-Wolfsen 2015; Brouwers & Kummeling 2016.

- Immuniteiten zijn niet toegestaan als zij de kern van het recht op toegang tot de rechter zonder goede reden aantasten (denk aan immuniteit bij strafvervolging van parlementariërs, militairen in het buitenland of ambassadepersoneel).
- Termijnen voor het instellen van beroep of hoger beroep mogen niet zo hoog zijn dat *de facto* geen toegang tot de rechter wordt geboden.[522]
- *Beoordeling van de volledige zaak* – de rechter moet 'full jurisdiction' hebben, wat betekent dat hij het voorgelegde geschil in zijn geheel moet kunnen beoordelen – wat overigens niet in de weg staat aan marginale toetsing van bestuursbesluiten.[523]
- *Tenuitvoerlegging* – de rechterlijke uitspraak moet daadwerkelijk en binnen redelijke termijn ten uitvoer worden gelegd; gebeurt dat niet, dan heeft de rechterlijke procedure immers geen enkel gevolg en is de toegang ertoe alsnog niet effectief.

II.4.3 Recht op een eerlijk proces

Het recht op toegang tot de rechter en een effectief rechtsmiddel hangt nauw samen met het recht op een eerlijk proces. Ook dit recht valt in een heel aantal deelrechten uiteen. Daarbij is van belang dat in de rechtspraak en in codificaties vaak onderscheid wordt gemaakt tussen procedurele rechten die gelden bij alle procedures – of die nu civielrechtelijk, bestuursrechtelijk of strafrechtelijk van aard zijn –[524] en bijzondere waarborgen die moeten worden geboden in het strafproces.[525] Voor dergelijke bijzondere waarborgen in het strafrecht is aanleiding, gelet op het machtsverschil dat zich daarbij voordoet tussen de staat (politie, openbaar ministerie, rechter-commissaris) en de verdachte. Hierna worden dan ook eerst enkele algemene waarborgen besproken; daarna komen enige specifieke strafrechtelijke waarborgen aan bod. Deze paragraaf beperkt zich daarbij tot die waarborgen die relevant zijn in relatie tot algoritme-gedreven besluitvorming.

Van de in de rechtspraak onderscheiden algemene procedurele waarborgen, zijn de volgende in het bijzonder relevant:

- *Redelijke termijn* – rechters moeten binnen redelijke termijn komen tot een afronding van hun procedures.[526] Om te beoordelen of aan dit vereiste is voldaan, wordt onder meer gekeken naar de complexiteit van de voorliggende rechtsvragen, naar het gedrag

522 Barkhuysen & Van Emmerik 2013, p. 217.
523 Zie met nadere verwijzingen Greer, Gerards & Slowe 2018, p. 360; Gerards, Barkhuysen & Van Emmerik 2014, p. 51.
524 Tot op zekere hoogte gelden de waarborgen bovendien niet alleen in de procedure voor de rechter, maar ook in bestuurlijke voorprocedures; zie o.m. De Jong 2017, p. 39-40.
525 Dat wil zeggen: als sprake is van een strafvervolging in de zin van art. 6 EVRM of art. 47 eerste zin Hv.
526 Zie nader en met verwijzingen naar relevante jurisprudentie o.m. Greer, Gerards & Slowe 2018, p. 361; De Jong 2017, p. 27-28; Widdershoven 2016.

van de procespartijen en naar het aantal instanties (beroep, hoger beroep) waarvoor een zaak heeft gespeeld. Wordt niet aan dit vereiste voldaan, dan moet daarvoor als zodanig weer effectief rechtsherstel worden geboden conform art. 13 EVRM; dat kan bijvoorbeeld de vorm krijgen van een schadevergoeding of bekorting of verlaging van een opgelegde straf.

- *Eerlijk, open en evenwichtig* – de procedure voor de rechter moet eerlijk en open verlopen, waarbij vooral de gelijkheid van de procespartijen (*equality of arms*) van groot belang is.[527] Geen van de partijen moet in een nadelige procespositie terechtkomen, bijvoorbeeld doordat de andere partij gemakkelijker toegang heeft tot bepaalde documenten of tot een deskundige, of doordat één partij niet wordt gehoord en de andere wel.[528] Anders gezegd moet er een zeker processueel evenwicht bestaan tussen de beide partijen.[529] Voor dit onderzoek relevante deelrechten die binnen het algemene vereiste van een eerlijk en open proces en *equality of arms* zijn erkend zijn de volgende:
- Beide partijen hebben het recht om te worden gehoord en moeten effectief kunnen reageren op elkaars stellingen (hoor en wederhoor).[530]
- Partijen moeten in gelijke mate in staat worden gesteld om voor de procedure relevant materiaal aan te dragen (deskundigenberichten, getuigenverklaringen, documenten).
- Er moet worden voorzien in faire en evenwichtige regels omtrent bewijs, bewijslast en bewijslastverdeling.
- Partijen moeten in gelijke mate en voldoende in staat worden gesteld om het voor de zaak relevante materiaal te bestuderen en te betwisten.[531] Dit impliceert niet alleen voldoende openbaarheid en transparantie van de stukken, maar ook voldoende voorbereidingstijd voor de beide partijen om er effectief op te kunnen reageren.[532] Daarnaast moeten voldoende mogelijkheden bestaan om de gronden te achterhalen en te begrijpen waarop een benadelende beslissing (zoals een sanctiebesluit) is gebaseerd.[533] Het recht op transparantie en openbaarheid van stukken is niet oneindig; sommige beperkingen (bijvoorbeeld ter bescherming van de nationale veiligheid of van bedrijfsbelangen)

527 Hier wordt niet apart ingegaan op het vereiste van een openbare behandeling en een openbare uitspraak; zie daarvoor o.m. De Jong 2017, p. 26-27.

528 Zie bijv. EHRM 7 juni 2001 (GK), nr. 39594/98, ECLI:CE:ECHR:2001:0607JUD003959498 (*Kress t. Frankrijk*), *EHRC* 2001/51 m.nt. A.W. Heringa, par. 72 en HvJ 6 november 2012, zaak C-199/11, ECLI:EU:C:2012:684 (*Otis*), *EHRC* 2013/3 m.nt. C. Mak, *NJ* 2013/168 m.nt. M.R. Mok, punt 71.

529 Greer, Gerards & Slowe 2018, p. 362; De Jong 2017, p. 32.

530 De Jong 2017, p. 30.

531 Greer, Gerards & Slowe 2018, p. 362.

532 Zie bijv. EHRM 20 september 2011, nr. 14902/04, ECLI:CE:ECHR:2011:0920JUD001490204 (*OAO Neftyanaya Kompaniya Yukos t. Rusland*), *EHRC* 2011/160, par. 538 e.v.

533 Gerards, Barkhuysen, & Van Emmerik 2014, p. 47; Greer, Gerards & Slowe 2018, p. 363. Zie bijv. HvJ EU 4 juni 2013, zaak C-300/11, ECLI:EU:C:2013:363, *EHRC* 2013/160 m.nt. A. Woltjer, *AB* 2013/374 m.nt. M. Reneman; HvJ EU 18 juli 2013, gev. zaken C-584/10 P, C-593/10 P en C-595/10 P, ECLI:EU:C:2013:518 (*Kadi*), *EHRC* 2013/229 m.nt. S.J. Hollenberg.

kunnen worden aanvaard, maar dat geldt alleen wanneer er goede redenen bestaan en de beperkingen daaraan evenredig zijn; ook moeten er dan compenserende waarborgen zijn om ervoor te zorgen dat in ieder geval de rechter zelf een volledig overzicht heeft van alle stukken en het geschil objectief en volledig kan beoordelen.
– *Motivering* – de rechterlijke uitspraak moet worden voorzien van een voldoende draagkrachtige motivering.[534] Dit betekent dat de belangrijkste aspecten van een zaak in ieder geval worden belicht, zodat het voor de partijen (eventueel bijgestaan door een advocaat) en een hogere rechter mogelijk is te begrijpen waarom een rechter tot zijn beslissing is gekomen. Welke eisen precies kunnen worden gesteld aan de motivering, is uiteindelijk alleen te beoordelen in de concrete context van de zaak waar het om gaat.[535]

Specifiek voor het strafrecht zijn de procedurele rechten vooral te vinden in art. 6 lid 2 en 3 EVRM; voor het EU-Grondrechtenhandvest staan ze in art. 48-50 Hv. Daarnaast zijn in de rechtspraak van het EHRM en het HvJ EU tal van rechten en verplichtingen terug te vinden die betrekking hebben op de voorfase van een strafrechtelijk onderzoek, bijvoorbeeld de inzet van specifieke opsporingsbevoegdheden waardoor inbreuk wordt gemaakt op de privacy. Deze waarborgen worden echter niet hier besproken, maar zijn kort aan de orde gekomen in paragraaf II.1. Voor dit onderzoek is vooral de onschuldpresumptie van belang: aangenomen wordt dat een verdachte onschuldig is, tot het tegendeel voldoende in rechte is komen vast te staan.[536] Dit betekent dat niet al tijdens de procedure besluiten mogen worden genomen of uitlatingen mogen worden gedaan waaruit blijkt dat de schuld van de verdachte al wordt aangenomen – stilzwijgend of expliciet. Rechters, politieagenten of rechters moeten dus voorzichtig zijn in hun uitlatingen jegens de media, maar ook bij het motiveren van beslissingen tot bijvoorbeeld voorlopige hechtenis of het motiveren van uitspraken in een bestuursrechtelijke zaak over een aanverwante kwestie.

534 Zie o.m. Gerards 2014; De Jong 2017, p. 33.
535 Zie voor strafzaken bijv. EHRM (GK) 29 november 2016, nr. 34238/09 (*Lhermitte t. België*), ECLI:CE:ECHR:2016:1129JUD003423809, *EHRC* 2017/52 m.nt. K. Lemmens en voor civiele zaken bijv. EHRM 24 oktober 2017, nrs. 57818/10, 57822/10, 57825/10, 57827/10 en 57829/10, ECLI:CE:ECHR:2017:1024JUD005781810 (*Tibet Mentes t. Turkije*), *EHRC* 2018/10.
536 Zie art. 6 lid 2 EVRM en de gelijkluidende bepaling van art. 48, eerste lid EVRM: 'Een ieder tegen wie een vervolging is ingesteld, wordt voor onschuldig gehouden totdat zijn schuld in rechte is komen vast te staan.' Zie voor de nadere uitwerking in de rechtspraak van het HvJ EU kort Greer, Gerards & Slowe 2018, p. 363-364.

III De (potentiële) impact van algoritmes op grondrechten in Nederland

III.1 Privacyrechten

III.1.1 Inleiding

Bij het beschrijven van knelpunten als gevolg van Big Data, het Internet of Things en Kunstmatige Intelligentie, komt het fundamentele recht op privacy veelal als eerste in beeld. In algemene zin geldt dat de algoritme-gedreven technologieën die in hoofdstuk I zijn omschreven, bij uitstek inbreuk kunnen maken op het privéleven van mensen.[537] Daarbij kunnen ook persoonlijke autonomie en menselijke waardigheid onder druk komen te staan. Als in hoofdstuk II uitgelegd zijn deze noties nauw verbonden met het klassieke vrijheidsrecht op privacy. Menselijke waardigheid, persoonlijke autonomie en privacy zijn grondrechten die niet vastomlijnd en soms lastig grijpbaar zijn. In deze paragraaf zal blijken dat van deze drie grondrechten, het recht op privacy het meest primaire grondrecht is voor situaties die samenhangen met nieuwe technologische ontwikkelingen.

In het hiernavolgende zal een breed palet aan (technologische) ontwikkelingen worden omschreven waarbij het recht op privacy, dan wel de daarmee verknoopte aspecten als de persoonlijke autonomie en menselijke waardigheid aan de orde (kunnen) komen. Achtereenvolgens zijn dat inbreuken door middel van surveillance, het gevaar van 'chilling effects' vanwege potentiële inbreuken op het recht op privéleven, enkele specifieke legaliteitsproblemen die zich kunnen voordoen bij opkomende technologische ontwikkelingen die de privacy bedreigen, robotisering en de samenhang met relationele privacy en menselijke waardigheid, de toenemende de-individualisering en de relatie daarvan met persoonlijke autonomie en menselijke waardigheid en ten slotte het recht om vergeten te worden.

III.1.2 Surveillance

'Big Data technologies, together with the sensors that ride on the Internet of Things, pierce many spaces that were previously private.'[538] Als gevolg hiervan zijn de overheid en

537 Zie Wagner 2017, p. 9.
538 White House 2014a, p. 53.

bedrijven steeds beter in staat zijn om een compleet beeld te krijgen van de levens van mensen en daarmee kunnen inbreuken op het recht op privéleven zich op steeds grotere schaal gaan voordoen. Kitchin geeft, onder verwijzing naar Koops, aan dat de gemiddelde Nederlander in honderden databases is opgenomen.[539] Deze databases bevatten niet enkele de digitale voetafdruk van deze personen (de informatie die zij over zichzelf achterlaten), maar ook hun 'dataschaduw', die bestaat uit alle informatie die door anderen over hen gegenereerd wordt. Deze verzameling van informatie resulteert in een zeer gedetailleerde weergave van het dagelijks leven van een individu. Onder meer zijn of haar consumptiepatroon, werk, reizen, communicatie met anderen, interactie met organisaties, interesses en onvervreemdbare karaktereigenschappen zijn allemaal in kaart gebracht. Het Internet of Things draagt eraan bij dat data wordt verzameld over voorheen ontoegankelijke delen van het privéleven van personen.[540] IoT-objecten kunnen (in theorie) een groot aantal fysieke en mentale gegevens van personen verzamelen, waaronder stressniveau, rookgewoontes, algeheel welzijn, de ontwikkeling van ziekten, slaappatroonen, geluk en lichamelijke inspanning. Op grond van deze opsomming is de conclusie dat 'loT devices could allow intrusive surveillance into the private spheres of individuals lives' zonder meer gerechtvaardigd.[541] Als beschreven in hoofdstuk I beperkt dataverzameling door IoT-objecten zich bovendien niet tot de medische of huiselijke sfeer, maar breidt deze zich uit tot dataverzameling in stedelijke omgevingen.[542] De voorgaande algoritme-gedreven ontwikkelingen raken daarmee inherent aan de persoonlijke levenssfeer van personen.[543] Volgens Wagner kan dit verstrekkende gevolgen hebben, omdat 'the use of algorithms (…) creates a risk of large-scale surveillance ('dataveillance') by private entities and governments alike.'[544]

Zoals beschreven in hoofdstuk II is het vaste rechtspraak van het EHRM dat surveillance uitgevoerd door de overheid, een inbreuk kan maken op het recht op privacy van burgers.[545] In recente rechtspraak maakt het EHRM duidelijk dat dit in het bijzonder het geval is in een sterk door nieuwe technologieën beheerste samenleving:

> '[T]he possibility occurring on the side of Governments to acquire a detailed profile of the most intimate aspects of citizens' lives may result in particularly

539 Kitchin 2014, p. 167. Zie ook Schermer & Wagemans 2009.
540 Ziegeldof, Morchon & Wehrle 2013, p. 2736.
541 Poudel 2016, p. 1013-1014.
542 Over de potentiële indringendheid daarvan, zie Van Zoonen 2016, p. 475-476.
543 Zie hierover onder meer Van den Hoven van Genderen 2017, p. 5.
544 Wagner 2017, p. 10.
545 De rechtspraak van het EHRM ziet vooral op 'secret surveillance' door veiligheidsdiensten. Zie daarover Harris e.a. 2014, p. 555-557. In deze alinea wordt specifiek ingegaan op de onderdelen van deze rechtspraak die relevant zijn in de context van Big Data en het IoT.

> invasive interferences with private life. This threat to privacy must be subjected to very close scrutiny both on the domestic level and under the Convention.'[546]

'Dataveillance' kan aldus een ernstige inbreuk op artikel 8 EVRM opleveren, die streng moet worden getoetst. Dit geldt te meer als daarbij gebruik wordt gemaakt van nieuwe technologieën:

> 'Any State claiming a pioneer role in the development of new technologies bears special responsibility for striking the right balance in this regard.'[547]

Daarbij is het van belang dat het recht op privacy zich, zoals reeds in hoofdstuk II aangegeven, ook kan uitstrekken tot de publieke ruimte. In *P.G. & J.H. t. het Verenigd Koninkrijk* sprak het EHRM van het bestaan van

> 'a zone of interaction of a person with others, even in a public context, which may fall within the scope of 'private life. (…) Private-life considerations may arise, (…) once any systematic or permanent record comes into existence of such material from the public domain. It is for this reason that files gathered by security services on a particular individual fall within the scope of Article 8, even where the information has not been gathered by any intrusive or covert method.'[548]

Dit maakt duidelijk dat het gebruik van data die verbonden zijn aan personen, bijvoorbeeld data verzameld in een slimme stad, een inbreuk op kan leveren op het recht op respect voor het privéleven en moet voldoen aan de eisen die art. 8 EVRM aan een dergelijke beperking stelt.[549]

---

546 EHRM 12 januari 2016, nr. 37138/14, ECLI:CE:ECHR:2016:0112JUD003713814 (*Szabó en Vissy t. Hongarije*), *NJB* 2016/641, par. 70. In de uitspraak verwijst het EHRM naar de uitspraak van het HvJ EU 8 april 2014, zaak C-293/12 en C-594/12, ECLI:EU:C:2014:238 (*Digital Rights Ireland*), *EHRC* 2014/140 m.nt. M.E. Koning, *NJ* 2016/446 m.nt. E.J. Dommering, par. 27 waarin wordt gewezen op de aanwezigheid van dataverzamelingen die 'taken as a whole, may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them.'

547 EHRM (GK) 4 december 2008, nrs. 30562/04 en 30566/04, ECLI:CE:ECHR:2008:1204JUD003056204 (*S. en Marper t. het Verenigd Koninkrijk*), *EHRC* 2009/13 m.nt. B.J. Koops, *NJ* 2009/410 m.nt. E.A. Alkema, par. 112.

548 EHRM 25 september 2001, nr. 44787/98, ECLI:CE:ECHR:2001:0925JUD004478798 (*P.G. en J.H. t. Het Verenigd Koninkrijk*), par. 56-57.

549 Zie hierover De Hert & Lammerant 2016, p. 153-154.

Als omschreven in hoofdstuk I is het bovendien niet alleen de overheid, maar zijn het (vooral) ook private actoren die een inbreuk kunnen plegen op het recht op privacy. Dat geldt ook voor situaties waarbij bepaalde bedrijven burgers aan surveillance onderwerpen. In het kader van dit onderzoek is vooral de rolvan het Internet of Things in horizontale verhoudingen relevant. Ter illustratie kan daarbij worden gewezen op de in hoofdstuk I omschreven 'smart devices' voor persoonlijke gezondheid. Van Est en Gerritsen wijzen erop dat werkgevers het dragen van een dergelijk object (in theorie) kunnen stimuleren of verplichten om de activiteiten van werknemers op het werk bij te houden.[550] Datzelfde geldt voor verzekeraars die verzekeringsnemers stimuleren om een *e-health*-armband te dragen. In ruil voor een premieverlaging kunnen verzekeraars dan gegevens over de fysieke gesteldheid van verzekeringsnemers monitoren.[551] Het EHRM heeft meermaals aangenomen dat surveillance ook in horizontale rechtsverhoudingen een inbreuk op artikel 8 EVRM op kan leveren. Zo oordeelde het Hof dat video-surveillance door een verzekeraar 'constituted processing or use of personal data of a nature to constitute an interference with [the] respect for private life.[552] Hetzelfde geldt voor het monitoren van privécommunicatie op de werkvloer.[553] Recente rechtspraak maakt duidelijk dat het hierbij niet uitmaakt of videosurveillance heimelijk geschiedt. Ook in een zaak waarin sprake was van kenbare videosurveillance in hoorcollegezalen, nam het Hof een schending van artikel 8 EVRM aan.[554] In het licht van deze rechtspraak levert het stimuleren of verplichten van het dragen van *e-health wearables* onvermijdelijk een privacyrechtelijk knelpunt op. Dit is vooral zo doordat het beeld van een persoon dat surveillance door *smart devices* oplevert, vele malen completer is dan het beeld dat – bijvoorbeeld – door middel van videosurveillance kan worden verkregen. In dit verband kunnen uit art. 8 EVRM positieve verplichtingen voortvloeien voor de verdragsstaten om nieuwe technologieën nader te reguleren om zodoende inbreuken op het privéleven te voorkomen. Ook kan in de (Nederlandse) rechtspraak gebruik worden gemaakt van het leerstuk van (indirecte) horizontale werking door in een civielrechtelijk geschil tussen burgers (particulieren) onderling het recht op privéleven als een zwaarwegend belang te laten meewegen. Gedacht kan bijvoorbeeld worden aan het plegen van een onrechtmatige daad (art. 6:162 BW), indien een derde gebruik maakt van gegevens door middel van onrechtmatige surveillance.[555]

---

550 Van Est & Gerritsen 2017, p. 24.

551 Ook dit scenario is niet denkbeeldig. Zie https://www.volkskrant.nl/wetenschap/hoe-zorgverzekeraars-gezonde-mensen-willen-belonen-geef-ze-een-smartwatch~a4512293/ (laatst geraadpleegd 22 februari 2018).

552 EHRM. 18 oktober 2016, nr. 61838/10, ECLI:CE:ECHR:2016:1018JUD006183810 (*Vukota-Bojić t. Zwitserland*), *EHRC* 2017/33, m.nt. F.G. Laagland.

553 EHRM (GK) 5 september 2017, nr. 61496/08, ECLI:CE:ECHR:2017:0905JUD006149608 (*Bărbulescu t. Roemenië*), *EHRC* 2018/3 m.nt. B.P. ter Haar, *JAR* 2017/259 m.nt. C.M. Jakimovicz.

554 EHRM 28 november 2017, nr. 70838/13, ECLI:CE:ECHR:2017:1128JUD007083813 (*Antović en Mirković t. Montenegro*), *JAR* 2018/20, para. 44.

555 Vgl. HR 9 januari 1987, *NJ* 1987/928 (*Edamse bijstandsmoeder*).

Situaties als in deze paragraaf omschreven zijn overigens ook in gezagsrelaties tussen burger en overheid niet ondenkbeeldig. Het in hoofdstuk I aangehaalde voorstel om jeugdige delinquenten *wearables* te laten dragen om hartslag, huidgeleiding en ademhaling te meten, levert in het licht van het voorgaande een grondrechtelijk knelpunt op.

III.1.3 'Chilling effects', autonoom denken en autonoom handelen

Een ander risico dat samenhangt met het recht op privacy en de opkomst van technologische ontwikkeling zijn de 'chilling effects' en de bedreiging voor het autonoom handelen van personen. Alvorens daar langer bij stil te staan volgt eerst iets over het begrip 'chilling effects'.

In 1791 beschreef Bentham het Panopticon; een ronde gevangenis bestaande uit een toren bemand door een bewaker, met daaromheen een ring van cellen.[556] Iedere cel heeft een groot glazen raam, dat uikijkt op de toren. De gevangenen kunnen de toren zien, waardoor zij weten dat ze op ieder moment in de gaten gehouden kunnen worden, maar zien niet of de bewaker hen in de gaten houdt. Hierdoor zullen gevangenen zich constant bewust zijn van hun gedrag. Zij zullen 'gewenst' gedrag vertonen om aan sanctionering door de bewaker te ontkomen. Benthams Panotpicon heeft een disciplinerende werking, die ook wel kan worden aangeduid als 'chilling effect'. Het Panopticon wordt vaak in verband gebracht met de in de vorige paragraaf omschreven surveillance door Big Data en het Internet of Things.[557] De wetenschap dat grote hoeveelheden data over hen worden opgeslagen en geanalyseerd kan het gedrag van personen beïnvloeden.[558] In de woorden van de WRR:

> 'mensen zullen zich als gevolg van deze continue dataverzameling op een andere manier gaan gedragen. Sommigen zullen hun gedrag aanpassen om zo normaal mogelijk te lijken, anderen zullen wellicht zoveel mogelijk buiten beeld proberen te geraken. In beide gevallen wordt hun vrijheid ingeperkt.'[559]

Ook emotieherkenning kan daarbij een invloedrijke rol spelen, bijvoorbeeld wanneer deze wordt ingezet om de openbare orde te handhaven bij grote evenementen of demonstraties. De wetenschap dat accurate emotieherkenning mogelijk is, kan ertoe leiden dat personen proberen hun gelaatsuitdrukking aan te passen. Het streven naar normconform gedrag

556 Bentham 1791.
557 Zie o.a. Zuiderveen Borgesius 2014, p. 111.
558 Van den Hoven van Genderen 2017, p. 11.
559 WRR 2016, p. 92. Dit *chilling effect* wordt breed erkend. Zie o.a. Lodder & Schuilenburg 2016, p. 152-153 met betrekking tot predictive policing en *webcrawlers* en Van Hout 2017, p. 1040 in de context van Big Data toepassingen door de Belastingdienst.

beperkt zich niet tot de publieke ruimte, maar strekt zich met de opkomst van het Internet of Things, uit tot in de huiskamers van mensen.[560] Dit streven wordt versterkt wanneer personen worden geconfronteerd met de gevolgen die algoritmes verbinden aan de (online) gedragingen van een persoon. Een bekend voorbeeld in dit geval ziet op *behavioural targeting,* waarbij advertenties worden afgestemd op eerder onlinegedrag. Zo bepaalde een 'pregnancy prediction algorithm' de kans dat een consument zwanger was, om daarop vervolgens advertenties aan te passen. Op basis van deze score, stuurde de winkel een zwanger tienermeisje kortingsbonnen voor zwangerschaps- en babyproducten toe. Doordat de vader van het meisje dergelijke bonnen op de deurmat vond, kwam hij erachter dat zijn dochter zwanger was. Dit voorbeeld illustreert dat intieme persoonskenmerken en persoonlijke omstandigheden – variërend van seksuele oriëntatie tot dreigende scheidingsproblematiek en financiële problemen – kunnen worden afgeleid uit on- en offlinegedrag en ten grondslag kunnen worden gelegd aan *behavioural targeting*.[561] Dit fenomeen beperkt zich bovendien niet tot het *behavioural targeting* of commerciële toepassingen in den brede. Het gegeven dat Big Data-analyse aan bepaalde zoekslagen of gezichtsuitdrukkingen consequenties kan verbinden, kan ook vergaande gevolgen hebben in het veiligheidsdomein. Kortom, de wetenschap dat surveillance alomtegenwoordig is, kan leiden tot 'chilling effects'. Deze effecten worden belangrijker als Big Data en het IoT een dominantere rol krijgen in het dagelijks leven van mensen.

*Chilling effect*s worden veelal gerelateerd aan het recht op vrijheid van meningsuiting,[562] maar komen in de rechtspraak van het EHRM ook naar voren bij klachten gestoeld op artikel 8 EVRM. Het bestaan van een *chilling effect* kan voldoende reden zijn om als slachtoffer in de zin van artikel 34 EVRM te worden aangemerkt.[563] Ook in de rechtspraak van het Hof van Justitie wordt, in rechtspraak over art. 7 en 8 van het Handvest, gewezen op de mogelijkheid van *chilling effects*.[564] De potentiële grondrechtelijke gevolgen van *chilling effects* doen zich eveneens voor in relatie tot persoonlijke autonomie. Zoals gebleken is in hoofdstuk II, heeft het EHRM persoonlijke autonomie gedefinieerd als 'the ability to conduct one's life in a manner of one's own choosing'.[565] Gedragsaanpassing ten gevolge

560 Poudel 2016, p. 1013: 'Just as the widespread use of CCTV has influenced people's behavior in public spaces, IoT may pressure people to avoid behavior that can be perceived as anomalous even in the comfort of their homes.'

561 King & Forder 2016, p. 702.

562 Zie daarover nader paragraaf 3 van dit hoofdstuk.

563 Van der Sloot 2016, p. 423-426.

564 HvJ 8 april 2014, gev. zaken C-293/12 en C-594/12, ECLI:EU:C:2014:238 (*Digital Rights*), *EHRC* 2014/140 m.nt. M.E. Koning, *NJ* 2016/446 m.nt. E.J. Dommering, par. 37: 'the fact that data are retained and subsequently used without the subscriber or registered user being informed is likely to generate in the minds of the persons concerned the feeling that their private lives are the subject of constant surveillance.'

565 EHRM 29 april 2002, nr. 2346/02, ECLI:CE:ECHR:2002:0429JUD000234602 (*Pretty t. het Verenigd Koninkrijk)*, *NJ* 2004/543, m.nt. E.E.A. Alkema, *EHRC* 2002/47, m.nt. J.H. Gerards & H.L. Janssen, par. 62.

van het *chilling effect* van Big Data en het IoT levert in het licht van deze definitie een knelpunt op in de uitoefening van het recht op persoonlijke autonomie. *Chilling effects* zijn een specifieke manifestatie van een breder gevolg van Big Data en het IoT: dit gevolg houdt in dat de mogelijkheid om autonoom te denken en te handelen door deze technologieën negatief kan worden beïnvloed. Zo stelt Richards dat surveillance negatief uitwerkt op:

> 'the ability (…) to develop ideas and beliefs away from the unwanted gaze or interference of others. Surveillance or interference can warp the integrity of our freedom of thought and can skew the way we think.'[566]

Een specifieke illustratie daarvan ziet op het vormen van een eigen smaak of mening. De Big Data-algoritmes die Facebook, Google, Netflix gebruiken bij het personaliseren van een nieuwsvoorziening of het aanbevelen van websites of films, kunnen onze mening en smaak in aanzienlijke mate beïnvloeden. De algoritmische aanbevelingen van Netflix en Spotify brengen bepaalde films en muziek onder de aandacht, hetgeen automatisch ten koste gaat van niet geprioriteerde films en muziek. Volgens Beer hebben algoritmes daarmee 'the capacity and potential to make taste by shaping cultural encounters and crafting our cultural landscapes.'[567] Hetzelfde geldt voor de vorming van een eigen mening. Gepersonaliseerde communicatie, die het gevolg is van de verzameling van grote hoeveelheden gegevens over het individu, zou de opvattingen en voorkeuren van mensen kunnen beïnvloeden, zonder dat ze dit doorhebben.[568] Hierbij kan (persoonlijke) autonomie bij het vormen van eigen opvattingen en keuzes onder druk komen te staan.[569] (Al dan niet ongemerkte) beïnvloeding van personen is niet louter een private aangelegenheid. Ook de overheid kan zich bedienen van digitale 'duwtjes in de goede richting' (*nudges*) bij de uitvoering van beleid.[570] Hierbij verdient ook het IoT bespreking. In een slimme omgeving die voortdurend anticipeert op de vermeende behoefte van zijn gebruikers, vermindert immers de ruimte voor het individu om eigen keuzes te maken. De optelsom van vele *nudges*, en personalisatietechnieken kan leiden tot een 'identiteitsparadox', waarbij het niet mensen zelf, maar algoritmes zijn die de identiteit van individuen vormgeven en zijn of haar keuzes bepalen:

> '[W]e lack the power to individually say who "I am," if filters and nudges and personalized recommendations undermine our intellectual choices. [W]e will

566 Richards duidt deze vrijheid aan als 'intellectual privacy'. Zie Richards 2008, p. 389.
567 Beer 2013, p. 99.
568 Zuiderveen Borgesius e.a. 2016, p. 260 en hierover nader paragraaf 3 over vrijheidsrechten.
569 Zie hierover ook Zarsky 2013, p. 35-40.
570 Zie Evers 2016.

> have become identified but lose our identities as we have defined and cherished them in the past.'[571]

De vraag die in het licht van de door het EHRM gehanteerde definitie van persoonlijke autonomie opkomt is, hoe personen naar eigen inzicht invulling geven aan hun leven, als sociale media en IoT-objecten ingezet door bedrijven en de overheid hen (al dan niet subtiel) in de richting van bepaalde voorkeuren, keuzes en gedragingen duwen? Daarmee krijgt een eerder door het Rathenau instituut geformuleerd bezwaar een grondrechtelijke connotatie.[572]

De hiervoor omschreven knelpunten raken ten slotte ook aan de vrijheid van godsdienst. Dit recht omvat immers de vrijheid de eigen (religieuze) overtuigingen en het eigen geweten zelf te bepalen (*forum internum*).[573] Als *chilling effects* ertoe leiden dat personen zich niet langer vrij voelen om hun eigen geweten en godsdienst te bepalen en ook de religieuze identiteit en innerlijke geestelijke vrijheid van personen beïnvloeden, komt de vrijheid van godsdienst onder druk te staan.[574]

III.1.4 Legaliteit en inbreuken op het recht op privacy

Als omschreven in hoofdstuk II, behoeven inbreuken op privacy een wettelijke basis. Daarbij verdient met name de materiële beperkingseis van art. 8, tweede lid EVRM aandacht. Bij de vraag of een inbreuk bij wet voorzien is, besteedt het EHRM onder meer aandacht aan de 'quality of the law'. De regelgeving waarbij een inperking van het recht op privacy is voorzien, moet voldoende 'safeguards against arbitrariness' bieden. Bij de inzet van moderne technologieën die kunnen resulteren in beperkingen van het recht op privacy, is deze legaliteitseis bijzonder relevant. Zo oordeelde het EHRM in de eerder aangehaalde zaak over video-surveillance door een verzekeraar, dat:

> '[i]n view of the risk of abuse intrinsic to any system of secret surveillance, such measures must be based on a law that is particularly precise, especially as the technology available for use is continually becoming more sophisticated.'[575]

---

571 Richards & King 2013, p. 44.

572 Van Est & Gerritsen 2017, p. 23.

573 Zie Van den Heede 2015 onder verwijzing naar o.a. ECieRM 15 december 1983, nr. 10358/83, DR 37, p. 142 (*C. t. het Verenigd Koninkrijk*): 'Article 9 primarily protects the sphere of personal beliefs and religious creeds, i.e. the area which is sometimes called the forum internum.'

574 Bezwaren gerelateerd aan het *forum externum* worden in paragraaf III.3 kort aangestipt.

575 EHRM 18 oktober 2016, nr. 61838/10, ECLI:CE:ECHR:2016:1018JUD006183810 (*Vukota-Bojić t. Zwitserland*), *EHRC* 2017/33 m.nt. F.G. Laagland, par. 67. Zie in dit kader ook EHRM 24 april 1990, nr. 11801/85,

Daarbij moet worden aangetekend dat de eisen die aan regelgeving worden gesteld afhangen van de indringendheid van een inbreuk op privacy. In de rechtspraak is nog geen antwoord gegeven op de vraag hoe bijvoorbeeld datamining en profileertechnieken in dit kader geclassificeerd moeten worden.[576] Wel zijn door enkele auteurs kritische kanttekeningen geplaatst bij de inzet van onder meer datamining en het IoT ten behoeve van de opsporing van strafbare feiten. Brinkhoff wijst er bijvoorbeeld op dat artikel 3 Politiewet een onvoldoende grondslag is voor de inzet politiële datamining. Zo behoeft de inzet van iColumbo een specifieke wettelijke grondslag.[577] Volgens Prins ontbreekt het op dit moment eveneens aan een adequate wettelijke grondslag voor de inzet van het IoT ten behoeve van de opsporing.[578]

III.1.4.1 Bescherming van de woning

In hoofdstuk II is omschreven dat het recht op eerbiediging van de woning wordt gegarandeerd door zowel de Grondwet, het EVRM, het EU-Grondrechtenhandvest en het IVBPR. De algemene constatering dat het IoT private actoren in staat stelt om bewoners constant te monitoren, raakt op zichzelf al aan het recht op de bescherming van de woning. Als de invloed van het IoT in woningen dusdanig dominant wordt, dat personen zich niet vrijelijk en naar eigen inzicht kunnen bewegen in hun woning, raakt dit nog indringender aan het recht op bescherming van de woning. Uit de rechtspraak van het EHRM volgt dat:

> 'breaches of the right to respect for the home are not confined to concrete or physical breaches, such as unauthorised entry into a person's home, but also include those that are not concrete or physical, such as noise, emissions, smells or other forms of interference.'[579]

Nadelige effecten van het IoT vallen daarmee potentieel binnen de reikwijdte van art. 8 EVRM en kunnen inbreuken veroorzaken op het recht op bescherming van de woning. Nu het IoT primair een private aangelegenheid is, is het van belang dat uit art. 8 EVRM positieve verplichtingen voor de staat kunnen voortvloeien om individuen te beschermen tegen verstoringen van de huisvrede.[580] Daarnaast kan wederom ook sprake zijn van indirecte horizontale werking in een civielrechtelijk geschil tussen burgers.

ECLI:CE:ECHR:1990:0424JUD001180185 (*Kruslin t. Frankrijk*), *NJ* 1991/523 m.nt. E.J. Dommering, par. 32.

576 Zie hierover Galetta & de Hert 2014.

577 Brinkhoff 2016 en Brinkhoff 2017.

578 Prins 2017. Het in de Wet Computercriminaliteit III opgenomen artikel 126nba Sv voorziet volgens Prins in een dergelijke grondslag. De wet is op dit moment in behandeling bij de Eerste Kamer.

579 EHRM 2 november 2006, nr. 59909/00, ECLI:CE:ECHR:2006:1102JUD005990900 (*Giacomelli t. Italië*), *AB* 2008/23 m.nt. T. Barkhuysen & M.L. van Emmerik, par. 76.

580 Gerards e.a. 2013, p. 145.

Koops en Prinsen wezen al eerder op het ontstaan van 'houses of glass', waarin het steeds beter mogelijk is om een beeld te krijgen van wat zich in een woning afspeelt, zonder deze binnen te treden. Zij dichten daarbij ook het IoT een rol toe.[581] Door zich – in het kader van de opsporing van strafbare feiten – toegang te verschaffen tot data verzameld door IoT-objecten, zou de overheid een gedetailleerd beeld kunnen krijgen van de levens van personen. Als in hoofdstuk II omschreven, biedt art. 12 Grondwet wel bescherming tegen het binnentreden van de woning door de overheid, maar komt dit grondrecht geen horizontale werking toe.[582] Hoewel de tekst van art. 12 Grondwet ogenschijnlijk enkel ziet op het fysiek binnentreden van de woning, blijkt uit de rationale van het artikel dat 'de bescherming tegen het onnodig en willekeurig binnentreden van een woning zonder toestemming niet omzeild mag worden door middel van technologie.'[583] In het licht van de grondwettelijke beperkingssystematiek is het van groot belang om een dergelijke inzet van het IoT, die een potentieel grote inbreuk kan maken op de bescherming van de huisvrede, te voorzien van een wettelijke basis, en indien gebruik wordt gemaakt van de delegatiemogelijkheid, de regeling voldoende specifiek toe te snijden op een inbreuk op het huisrecht.[584]

III.1.4.2 Lichamelijke integriteit

Art. 11 Gw, art. 8 EVRM, art. 3 Hv en art 17 IVBPR beschermen het recht op lichamelijke integriteit. In dit verband kan op een aantal ontwikkelingen worden gewezen die een potentieel gevaar kunnen vormen voor het recht op lichamelijke integriteit. Voortschrijdende technologische ontwikkelingen maken het bijvoorbeeld mogelijk om de sensoren van het IoT dusdanig te verkleinen dat deze ook *in* het menselijk lichaam geplaatst kunnen worden.[585] De inzet van deze technologieën leidt ertoe dat het lichaam in toenemende mate transparant wordt.[586] Voor zover IoT-objecten van nano-formaat in het lichaam worden gebracht, staat dit op gespannen voet met art. 11 Gw. Dergelijke inbreuken, wanneer van overheidswege voorgeschreven, moeten worden voorzien van een wettelijke basis. Gezien de materiële beperkingssystematiek van het EVRM en EU-Grondrechtendhandvest, moet voor verdere bescherming vooral naar deze instrumenten worden gekeken. Indien er sprake is van een privaatrechtelijke speler kan bovendien sprake zijn van horizontale werking van art. 11 Gw.[587]

---

581 Koops & Prinsen 2007, p. 180.

582 Het arrest van het Hof Amsterdam 8 januari 1998, *NJ* 2000/152, waarin een dergelijke werking wel werd aangenomen, is een staatsrechtelijke eendagsvlieg.

583 Buisman & Kierkels 2013.

584 ABRvS 28 augustus 1995, *AB* 1996/204 (*Drugspand Venlo*).

585 Zie hoofdstuk I, paragraaf 3.3.

586 Zie hierover Koops & Prinsen 2007, p. 184-185 en Perry & Roda 2017, p. 67.

587 Zie hierover o.a. Koops 2009, p. 289 en eveneens een klassiek arrest van de Hoge Raad waar een zeldzame variant van *directe* horizontale werking werd toegepast: HR 18-06-1993, *NJ* 1994/347 (*Verplichte aidstest*). Directe horizontale werking betekent dat het grondrecht (hier art. 11 Gw) in een privaatrechtelijk geschil werkt op eenzelfde wijze als in een verticale relatie. Dat wil zeggen dat eerst de reikwijdte van het grondrecht

III.1.5 Robots, relationele privacy en menselijke waardigheid

Het recht op respect voor privéleven is niet enkel een negatief afweerrecht tegen onwenselijke inbreuken op welzijn en integriteit, maar kent ook een positieve component die inhoudt dat een persoon de eigen persoonlijkheid en identiteit vorm moet kunnen geven.[588] Artikel 8 EVRM omvat daarmee, zoals in hoofdstuk II eveneens aangegegeven

> 'the right to establish and to develop relationships with other human beings, especially in the emotional field for the development and fulfilment of one's own personality.'[589]

Hieruit volgt dat het

> 'right to a private social life (…) enshrines the possibility of approaching others in order to establish and develop relationships with them.'[590]

De opkomst van robots in vele maatschappelijke domeinen roept in dit kader vragen op. Zo kan de uitoefening van dit recht problematisch zijn voor kwetsbare groepen als kinderen, zieken, ouderen of gehandicapten. Zij zijn voor het aangaan van relaties met andere mensen soms afhankelijk van hun omgeving, veelal in de vorm van verpleging of zorg. In hoofdstuk I is gewezen op de opkomst van met KI uitgeruste zorgrobots die kunnen voorzien in de zorg van deze kwetsbare groepen. De vraag is in hoeverre dergelijke robots mogen worden ingezet ter vervanging van menselijke verplegers.[591] Naast de ethische constatering dat '[b]eing somehow forced to consider digital media and inanimate objects as the comprehensive universe of one's own social life may become humiliating and may hurt self-respect',[592] is bij de inzet van zorgrobots immers mogelijk ook het recht op een 'private social

---

wordt bepaald , waarna een grondslag voor een eventuele beperking dient te worden gevonden in een formele wet, veelal art. 6:162 BW.

588 Zie tevens hoofdstuk II, alwaar is verwezen naar Greer, Gerards & Slowe 2018, p. 165

589 ECieRM 8 mei 1976 nr. 6825/74, 5 DR 86 at 88 (*Commissie X t. IJsland*). Zie ook EHRM 16 december 1992, nr. 13710/88, ECLI:CE:ECHR:1992:1216JUD001371088 (*Niemietz t. Duitsland*), *NJ* 1993/400 m.nt. E.J. Dommering en EHRM (GK) 5 september 2017, nr. 61496/08, ECLI:CE:ECHR:2017:0905JUD006149608 (*Bărbulescu t. Roemenië*), *EHRC* 2018/3 m.nt. B.P. ter Haar, *JAR* 2017/259 m.nt. C.M. Jakimovicz, par. 70-73.

590 EHRM (GK) 5 september 2017, nr. 61496/08, ECLI:CE:ECHR:2017:0905JUD006149608 (*Bărbulescu t. Roemenië*), *EHRC* 2018/3 m.nt. B.P. ter Haar, *JAR* 2017/259 m.nt. C.M. Jakimovicz., para. 70–73, EHRM 28 mei 2009, nr. 26713/05, ECLI:CE:ECHR:2009:0528JUD002671305 (*Bigaeva t. Griekenland*), *EHRC* 2009/88, m.nt. S. Claessens. para. 22 en EHRM 19 oktober 2010, nr. 20999/04, ECLI:CE:ECHR:2010:1019JUD002099904 (*Özpinar t. Turkije*), *EHRC* 2011/5 m.nt. Barkhuysen & De Jong para. 45.

591 Van Est & Gerritsen 2017, p. 25. Zie ook European Research Cluster on the Internet of Things 2015, p. 22-23.

592 Mordini e.a. 2009, p. 203–220. Zie eveneens, veelal onder verwijzing naar menselijke waardigheid, Sharkey 2014 en Laitinen, Niemelä & Pirhonen 2016.

life' in het geding. De inzet van zorgrobots kan een inbreuk op artikel 8 EVRM opleveren, als hierdoor de mogelijkheid om relaties met andere personen te ontwikkelen negatief wordt beïnvloedt.[593] Daarbij speelt ook de mogelijk veranderende houding van de omgeving van zorgbehoevenden een rol. De opkomst van zorgrobots kan ertoe leiden dat vrienden en familie denken 'maak je maar geen zorgen om oma; de robot houdt haar wel gezelschap.'[594]

Een ander grondrechtelijk knelpunt bij de inzet van robots is gerelateerd aan de menselijke waardigheid. Menselijke waardigheid speelt in de rechtspraak van het EHRM, met name en rol bij de uitleg van de rechten in het EVRM.[595] De opkomst van robots kan leiden tot vragen over de uitleg van deze rechten. Zo kunnen zorgrobots die verbaal of fysiek aandringen op het nemen van medicijnen door patiënte leiden tot vernederende behandeling.[596] Dergelijke vragen komen nog pregnanter naar voren bij autonome wapensystemen, die zelfstandig mensen kunnen doden. Er bestaat 'widespread concern that allowing Lethal Autonomous Robotics to kill people may denigrate the value of life itself.'[597] Bij de interpretatie van art. 2 en 3 EVRM is daarmee ook menselijke waardigheid in het geding.

III.1.6 De-individualisering, persoonlijke autonomie en menselijke waardigheid

Ondanks het streven van Big Data naar volledige dataverzamelingen (*n=all*), is het onmogelijk om alle gegevens over een persoon te verzamelen. Besluitvorming op basis van Big Data-analyse baseert zich op de wel beschikbare gegevens over personen. Deze gegevens zijn per definitie niet volledig, bijvoorbeeld omdat karaktereigenschappen of emoties niet gedigitaliseerd kunnen worden. Custers geeft aan dat wanneer Big Data ten grondslag wordt gelegd aan besluitvorming, 'het belang van iemands digitale persoonlijkheid toeneemt'.[598] Op basis van deze, niet volledig representatieve, digitale persoonlijkheid worden beslissingen genomen over echte mensen. Niet het individu, maar zijn of haar digitale representatie komt daarmee centraal te staan bij besluitvorming. Ook op een aanverwante manier staat de positie van het individu bij besluitvorming onder druk. Profileren kan worden ingezet voor het opstellen van groepsprofielen, die bestaan uit een verzameling attributen van een groep personen. Als gevolg van profilering kunnen beslissingen over

593 Daarbij moet worden aangetekend dat zorgrobots uiteraard ook kunnen dienen ter bevordering van menselijk conctact, bijvoorbeeld doordat zij bijdragen aan het vergroten van de mobiliteit van zorgbehoevenden.
594 Koops e.a. 2013 onder verwijzing naar Sharkey & Sharkey 2010.
595 Buyse 2016.
596 Van Est & Gerritsen 2017, p. 25.
597 UN Special Rapporteur on extrajudicial, summary or arbitrary executions 2013, p. 20, para. 109.
598 Custers 2017, p. 33.

individuen worden genomen, gebaseerd op de groep waartoe zij behoren. Profileren leidt er daarmee toe dat 'persons are judged on the basis of group characteristics rather than on their own individual characteristics and merits.'[599] Big Data kan zo leiden tot besluitvorming die tweevoudig van het individu verwijderd is. Niet de echte persoon, maar zijn of haar digitale persoonlijkheid is van belang. En niet de individuele digitale persoonlijkheid staat centraal, maar de groep waartoe deze persoonlijkheid behoort op basis van zijn of haar attributen.

De-individualisering als gevolg van Big Data kan op gespannen voet staan met de bescherming van menselijke waardigheid en persoonlijke autonomie. Uit EHRM-rechtspraak volgt dat persoonlijke autonomie een funderend beginsel is aan de hand waarvan het recht op respect voor het privéleven moet worden uitgelegd.[600] In *Goodwin t. het Verenigd Koninkrijk* oordeelde het EHRM:

> 'Under Article 8 of the Convention in particular, where the notion of personal autonomy is an important principle underlying the interpretation of its guarantees, protection is given to the personal sphere of each individual, including the right to establish details of their identity *as individual human beings*.'[601]

Besluitvorming slechts gebaseerd op de groep waartoe de digitale persoonlijkheid van een persoon behoort, kan een knelpunt opleveren bij de uitoefening van het recht om als 'individual human being' een eigen identiteit vorm te geven. Dat wordt met name problematisch als een persoon waardevolle opties worden ontzegd op basis van dergelijke besluiten. Dan speelt ook menselijke waardigheid een rol. In de rechtspraak zijn nog geen directe voorbeelden met betrekking tot dit vraagstuk voorhanden. Wel kan in dit verband worden gewezen op de Conclusie van A-G Maduro in de zaak *Coleman*, waarin nader wordt ingegaan op de 'waarden' van persoonlijke autonomie en menselijke waardigheid die ten grondslag liggen aan het recht op gelijke behandeling.[602] Het beschermen van autonomie en menselijke waardigheid betekent volgens Maduro dat mensen niet op grond

599 Schermer 2011, p. 4. Zie ook Vedder 1999, p. 275.

600 EHRM (GK) 11 juli 2002, nr. 28957/95, ECLI:CE:ECHR:2002:0711JUD002895795 (*Christine Goodwin t. het Verenigd Koninkrijk*), *EHRC* 2002/74 m.nt. H.L. Janssen & J. van der Velde. Zie ook EHRM 29 april 2002, nr. 2346/02, ECLI:NL:XX:2002:AP0678 (*Pretty t. VK*), *EHRC* 2002/47 (m.nt. Gerards en Janssen), *NJ* 2004/543 m.nt. E.A. Alkema, *NJCM-Bull.* 2002, p. 910 m.nt. B.E.P. Myjer, par. 61.

601 EHRM (GK) 11 juli 2002, nr. 28957/95, ECLI:CE:ECHR:2002:0711JUD002895795 (*Christine Goodwin t. het Verenigd Koninkrijk*), *EHRC* 2002/74 m.nt. H.L. Janssen & J. van der Velde, par. 90, onze cursivering. Zie ook EHRM 7 februari 2002, nr. 53176/99, ECLI:CE:ECHR:2002:0207JUD005317699 (*Mikulić t. Kroatie*), *EHRC* 2002/25 m.nt. H.L. Janssen, par. 54.

602 Conclusie A-G Maduro van 31 januari 2008, ECLI:EU:C:2008:61 bij HvJ 17 juli 2008, zaak C-303/06, ECLI:EU:C:2008:415 (*Coleman*), *EHRC* 2008/108 m.nt. A.C. Hendriks, *NJ* 2008/501 m.nt. Mok, TRA 2008 m.nt. Veldman.

van verdachte classificaties waardevolle opties, zoals toegang tot het arbeidsproces, mogen worden ontzegd op gebieden die van fundamenteel belang zijn voor hun leven.[603]

Zoals in paragraaf III.2.2 aan bod komt, verdienen profileertechnieken bijzondere aandacht vanuit het oogpunt van het recht op gelijke behandeling. Groepsprofielen kunnen immers gebaseerd zijn op verdachte discriminatiegronden als ras en geslacht, of daarmee verbonden zijn. Als op basis van een discriminatoir profiel beslissingen worden genomen ten aanzien van een individu, raakt dit ook aan de persoonlijke autonomie en menselijke waardigheid van een persoon.[604] In het licht van het voorgaande kan – ook in de afwezigheid van specifieke rechterlijke uitspraken op dit terrein – gesteld worden dat besluitvorming gebaseerd op Big Data grondrechtelijk problematisch kan zijn. Dergelijke besluitvorming gaat er immers aan voorbij 'dat elk mens uniek is en ook het recht heeft als zodanig gezien en behandeld te worden. Dit kan op gespannen voet staan met de menselijke waardigheid.'[605]

III.1.7 Het recht om vergeten te worden

Ten slotte is van belang hier stil te staan bij het recht op vergeten te worden. Uit het arrest *Google Spain* volgt dat betrokkenen, onder bepaalde voorwaarden, het recht hebben om zoekresultaten op basis van zoekslagen naar hun naam te laten verwijderen.[606] Dit recht is eveneens neergelegd in artikel 17 van de Algemene Verordening Gegevensbescherming.[607] Het 'right to be forgotten' is primair gerelateerd aan het gegevensbeschermingsrecht. Dit recht valt buiten de reikwijdte van dit rapport, maar het is van belang te erkennen dat het recht om vergeten te worden sterke raakvlakken vertoont met het recht op privacy, maar zeker ook met het algemeen persoonlijkheidsrecht zoals in hoofdstuk II omschreven. In *Google Spain* overwoog het HvJ dat de activiteiten van een zoekmachines het recht op privacy kunnen beperken wanneer:

> 'op de naam van een natuurlijke persoon wordt gezocht, aangezien elke internetgebruiker op basis van deze verwerking via de resultatenlijst een gestructureerd overzicht kan krijgen van de over deze persoon op het internet vindbare informatie, die potentieel betrekking heeft op tal van aspecten van zijn privéleven en die, zonder deze zoekmachine, niet of slechts zeer moeilijk met elkaar

603 Zie voor deze samenvatting van de Conclusie, Gerards, Koffeman & Hendriks 2013, p. 67.

604 Hierbij moet worden aangetekend dat de termen persoonlijke autonomie en menselijke waardigheid als zodanig niet in de uitspraak van het HvJ in Coleman voorkomen, 'waardoor uit dit arrest op dit punt geen bindende conclusies kunnen worden afgeleid,' zie Gerards, Koffeman & Hendriks 2013, p. 68.

605 Custers 2017, p. 33 onder verwijzing naar artikel 1 Hv.

606 HvJ EU 13 mei 2014, C-131/12, ECLI:EU:C:2014:317 (*Google Spain*), *EHRC* 2014/186, m.nt. J.V.J. van Hoboken, *NJ* 2014/385 m.nt. M.R. Mok.

607 In de Verordening wordt het recht aangeduid als het recht op 'gegevenswissing' of het 'recht op vergetelheid'.

> in verband had kunnen worden gebracht, en deze internetgebruiker aldus een min of meer gedetailleerd profiel van de betrokkene kan opstellen.'[608]

Het recht op bescherming van de persoonlijke levenssfeer omvat, als hiervoor besproken, volgens rechtspraak van het EHRM het recht om de eigen identiteit vorm te geven. Dit recht ziet ook op fundamentele persoonkenmerken als 'gender identification, name and sexual orientation.'[609]

Big Data en KI vormen aanzienlijke technologische uitdagingen voor de effectuering van het recht om vergeten te worden, juist in situaties waarin fundamentele persoonskenmerken als geslacht, religie of sexuele geaardheid in het geding zijn. Korenhof en Koops concludeerden dat het, gezien de grote hoeveelheden data die over personen worden verzameld, onmogelijk is om belangrijke identiteitskenmerken digitaal te verwijderen:

> 'the R2BF cannot control the extensive data flows relating to the core characteristics of a person's identity. The R2BF may be suited for having single actions, utterances, or events forgotten, but it will hardly help to have core identity-related characteristics, such as gender, religion, or race 'forgotten'.[610]

Dit probleem is in grotere mate aanwezig in de context van complexe informatiesystemen waarin KI, bijvoorbeeld in de vorm van ML, een rol speelt. Volgens Villaronga, Kieseberg en Li bestaat er bij het recht om vergeten te worden 'a clear disconnect between law and technical reality.' Deze discrepantie vloeit voort uit het feit dat, het recht om vergeten te worden is gebaseerd op concepties over het *menselijke vermogen* om te vergeten. 'Vergeten' is voor KI echter veel complexer; sterker nog: 'it may be impossible for AI to truly forget.'[611] De technologische moeilijkheden die zich voordoen bij de uitoefening van het recht om vergeten te worden, raken direct aan artikel 8 EVRM. Individuen hebben het recht om hun eigen identiteit vorm te geven, maar Big Data en KI leiden ertoe dat het recht om vergeten te worden lastig geëffectueerd kan worden. Daardoor wordt effectieve uitoefening van het recht om de eigen identiteit vorm te geven belemmert, juist als het gaat om fundamentele persoonskenmerken.

608 HvJ EU 13 mei 2014, C-131/12, ECLI:EU:C:2014:317 (*Google Spain*), *EHRC* 2014/186, m.nt. J.V.J. van Hoboken, *NJ* 2014/385 m.nt. M.R. Mok, par. 80.

609 Zie o.a. EHRM (GK) 4 december 2008, nrs. 30562/04 en 30566/04, ECLI:CE:ECHR:2008:1204JUD003056204 (*S. en Marper t. het Verenigd Koninkrijk*), *EHRC* 2009/13 m.nt. B.J. Koops, *NJ* 2009/410 m.nt. E.A. Alkema), par. 66.

610 Korenhof en Koop 2013.

611 Voor een verdere technologische uitwerking zie Villaronga, Kieseberg & Li 2017.

III.2 Gelijkheidsrechten

III.2.1 Inleiding

De opkomst van Big Data, mede gestimuleerd door het Internet of Things, kan het risico op discriminatie bij besluitvorming vergroten doordat de mogelijkheden tot differentiatie in de benadering, beoordeling of behandeling van groepen of personen toenemen.[612] Dergelijke differentiatie is problematisch vanuit het oogpunt van het discriminatieverbod als sprake is van ongerechtvaardigd onderscheid. Zoals nader besproken in hoofdstuk II is van discriminatie of ongerechtvaardigd onderscheid al snel sprake wanneer onderscheid wordt gemaakt op basis van 'verdachte' kenmerken als ras, geslacht of handicap; daarvoor is niet snel een rechtvaardiging te geven. Ook als een ongelijke behandeling of differentiatie niet rechtstreeks op een dergelijke grond is gebaseerd (indirecte discriminatie) kan die problematisch zijn. Ook dan moet de ongelijkheid immers steeds verklaarbaar zijn vanuit objectieve doelstellingen en moet de ongelijkheid proportioneel zijn aan het gestelde doel.

In grote lijnen geldt voor deze rechtvaardiging steeds dezelfde set van eisen: (1) redelijke grond van onderscheid, (2) legitieme doelstelling, (3) voldoende specifieke afbakening en geschiktheid om het doel te bereiken, (4) noodzakelijkheid van een besluit of regel om dit doel te bereiken, (5) redelijke verhouding tussen de belangenaantasting die het gevolg is van de ongelijke behandeling en het nagestreefde doel. Daarbij geldt dat deze eisen zwaarder worden wanneer de ongelijke behandeling direct of indirect is gebaseerd op een 'verdachte' grond, dat wil zeggen wanneer het bijvoorbeeld nadelig uitpakt voor een bepaalde etnische groep, voor mensen met een handicap, of voor mensen met een bepaalde seksuele gerichtheid.

Zoals in hoofdstuk II uitgelegd, gelden voor de verschillende categorieën van ongelijke behandeling echter steeds iets verschillende rechtvaardigingsmogelijkheden, afhankelijk van de vraag in welke context ze zich voordoen en welke codificatie van toepassing is. Bij directe discriminatie bij het aanbieden van goederen en diensten en bij ongelijke behandeling op de arbeidsmarkt stelt de Algemene wet gelijke behandeling (AWGB) bijvoorbeeld strenge eisen als de discriminatie op specifiek benoemde gronden is gebaseerd. Voor andere contexten of andere gronden gelden meer open regels, zoals die van artikel 1 Grondwet of artikel 14 EVRM. Om te beoordelen of een ongelijke behandeling te billijken is, moet per situatietype dan ook steeds worden onderzocht (a) welk type ongelijke behandeling

612 Zie hierover De Hert, Lammerant & Blok 2017. Hier moet direct bij worden aangetekend dat automatische besluitvorming discriminatie ook kan verminderen, doordat de dominantie van menselijke vooringenomenheid in besluitvorming afneemt. In het licht van het onderwerp van dit onderzoek, gaat de aandacht echter uit naar de mogelijk risico's die algoritme-gedreven technologieën vormen voor het recht op gelijke behandeling.

aan de orde is, (b) welke codificatie van toepassing is en (c) welke eisen deze bepaling (en de daarover bestaande rechtspraak) stelt.

Gelet hierop is het nauwelijks mogelijk om in deze paragraaf specifiek in te gaan op de vraag met welke specifieke gelijkheids- of non-discriminatiebepalingen bepaalde technologische toepassingen in strijd zouden kunnen zijn. Vanwege de overeenkomsten tussen deze bepalingen en gelet op het doel van dit onderzoek is dat ook niet nodig. Hierna wordt dan ook vooral inzicht geboden in het soort technologische toepassingen van algoritmegedreven besluitvorming dat op gespannen voet kan komen te staan met het verbod van discriminatie en het gelijkheidsbeginsel in algemene zin. In paragraaf III.2.2 wordt de relatie uiteengezet tussen de in hoofdstuk I omschreven technologieën en het gelijkheidsbeginsel en het recht op non-discriminatie. Daarbij worden eveneens voorbeelden gegeven van mogelijke discriminatie door Big Data-processen. In paragraaf III.2.3 komen mogelijke oorzaken van dergelijke discriminatie aan bod. In paragraaf III.2.4 worden enkele algemene grondrechtelijke aandachtspunten geïdentificeerd.

III.2.2 Differentiatie en discriminatie door Big Data-technieken

Vanuit het perspectief van het discriminatieverbod heeft automatische besluitvorming op het eerste gezicht de nodige voordelen. In hoofdstuk II is immers als gebleken dat veel discriminatie wordt veroorzaakt door menselijke vooringenomenheid en vooroordelen. Het idee is dat dit bij automatische besluitvorming wordt dit voorkomen door het inzetten van objectieve en neutrale algoritmes. Zoals omschreven in hoofdstuk I is de neutraliteit van algoritmes echter veelal schijn. Algoritmes die worden ingezet in een Big Data-context kunnen gebaseerd zijn op stereotypen of vooroordelen die kunnen leiden tot verboden onderscheid tussen individuen en groepen. In andere woorden: 'Big data techniques have the potential to enhance our ability to prevent discriminatory harm. But, if these technologies are not implemented with care, they can also perpetuate, exacerbate, or mask harmful discrimination.'[613]

Datamining en profilering verdienen in dit kader bijzondere aandacht.

– Datamining is inherent gericht op het maken van onderscheid tussen individuen. Zo brengen classificatie- en clustertechnieken individuen onder in verschillende groepen (bijvoorbeeld wel/geen terrorist) om vervolgens aan de hand van deze classificatie groepsgerichte beslissingen te nemen. Regressie-algoritmes resulteren in numerieke voorspellingen over individuele gebruikers (bijvoorbeeld voor wat betreft levensverwachting) en maken onderscheid op basis van deze voorspelling mogelijk. Hierbij

613 White House 2016, p. 5.

bestaat het gevaar dat (groepen van) individuen worden benadeeld op basis van verdachte gronden, zonder dat dit eenvoudig traceerbaar is.[614]
– Profilering kan leiden tot het opstellen van profielen die (indirect) verbonden zijn met verdachte discriminatiegronden als ras, geloof of seksuele gerichtheid.[615]

Het uiteindelijke doel van Big Data-processen is het omzetten van de uit analyse verkregen informatie naar *actionable knowledge*. Als private of overheidsactoren besluiten nemen op grond van verdachte gronden, verbanden of profielen, kan dit in strijd zijn met het gelijkheidsbeginsel. De mogelijke voorbeelden van dergelijke algoritmische besluiten zijn talrijk en strekken zich uit over een veelheid aan terreinen:
– Verzekeraars zijn in staat om onderscheid te maken in de hoogte van premies van verzekeringnemers aan de hand van een grote hoeveelheid aan factoren.[616] Informatie over onvervreemdbare kenmerken zal niet altijd in databases aanwezig zijn, maar op basis van wel beschikbare data kunnen algoritmes andere persoonskenmerken als ras of seksuele gerichtheid achterhalen.[617] Een algoritme kan relevante verbanden tussen deze eigenschappen opsporen en hierop de hoogte van de premie afstemmen. Door middel van een constant vergelijkingsproces met daadwerkelijk uitgekeerde vergoedingen, kan het algoritme dergelijke discriminerende verbanden zelflerend ontwikkelen en verfijnen. De opkomst van het Internet of Things verdient hierbij bijzondere aandacht. Data over de gezondheid van personen, bijvoorbeeld afkomstig van *wearables*, kan belangrijke informatie opleveren voor verzekeraars en de basis voor differentiatie vormen.[618]
– Werkgevers kunnen gebruik maken van algoritmes als basis voor besluitvorming en daarbij onderscheid maken tussen personen en groepen. Bij het aannemen van nieuw personeel zijn algoritmes bijvoorbeeld theoretisch in staat om een verband leggen tussen persoonskenmerken en het toekomstig succes van sollicitanten.[619] Dit zal op gespannen voet staan met het discriminatieverbod wanneer het hierbij gaat om verdachte kenmerken. Zo kan het automatisch matchen van cv's en functieomschrijvingen leiden tot discriminatie op grond van etniciteit, ook wanneer de etniciteit van sollicitanten als zodanig niet in de dataset voorkomt.[620] Het is onwaarschijnlijk dat hiervoor stelselmatig een objectieve en redelijke rechtvaardiging bestaat.

614 Barocas & Selbst 2016, p. 677.
615 WRR 2016, p. 112.
616 Zie infra Hoofdstuk I, para. 2.3 en verder Timmer e.a. 2015.
617 Denk hierbij aan het hierboven aangehaalde onderzoek waaruit blijkt dat Facebook in staat is om een aantal hoogstpersoonlijke eigenschappen van gebruikers te voorspellen op basis van beschikbare gegevens over deze gebruikers.
618 Peppet 2014, p. 33.
619 Rosenblat, Kneese & Boyd 2014, p. 10.
620 Žliobaitė & Custers 2016, p. 184.

- Banken en andere verstrekkers van leningen kunnen gebruik maken van algoritmische vaststellingen van kredietwaardigheid, waarbij bijvoorbeeld een lage kredietscore wordt toegekend aan personen met laagbetaalde banen. Als voornamelijk etnische minderheden of personen met een handicap dergelijke banen hebben, kan dit leiden tot indirecte discriminatie, waarvoor in ieder geval een objectieve en redelijke rechtvaardiging moet worden gevraagd.[621] Ook de praktijk van *redlining* is een voorbeeld van indirecte discriminatie. Financiële instellingen trekken hierbij rode lijnen om wijken waarin veel mensen met een slechte kredietscore wonen. Mensen in deze wijken krijgen vervolgens een lagere kredietscore. Wegens de nauwe verbondenheid tussen postcode, etniciteit en sociaaleconomische status worden hierdoor etnische minderheden veelal uitgesloten van toegang tot krediet.[622] Dit voorbeeld laat zien dat ogenschijnlijk neutrale gegevens als postcode dusdanig verbonden kunnen zijn met verdachte gronden dat het gebruik ervan in algoritmische besluitvorming kan leiden tot indirecte discriminatie.
- Marketingacties van bedrijven of verkoopaanbiedingen van webwinkels richten zich niet langer tot gehele populaties, maar kunnen steeds verder worden toegespitst op specifieke groepen die gekenmerkt worden door bijvoorbeeld een gemeenschappelijke opleiding of seksuele gerichtheid.[623] Is dit laatste het geval, dan kan sprake zijn van directe discriminatie; in het eerste geval kan indirecte discriminatie aan de orde zijn. Opnieuw hangt dit af van de vraag of in dit soort gevallen een toereikende rechtvaardiging voor de differentiaties kan worden gegeven.
- In het sociale zekerheidsdomein kan worden gedifferentieerd tussen bepaalde groepen werklozen. Het in hoofdstuk I besproken systeem dat hiertoe in Polen is ingevoerd, kan leiden tot ongerechtvaardigd onderscheid. Personen die bij een bepaalde categorie zijn ondergebracht, hebben slechts beperkt recht op ondersteuning bij het vinden van werk. Bij deze categorisering spelen leeftijd, geslacht of handicap een rol. Een ander relevant criterium is de vraag of de werkzoekende verantwoordelijk is voor de opvoeding van kinderen. Een systeem als dit kan leiden tot indirecte discriminatie, doordat vrouwen relatief vaker de zorg voor een kind op zich nemen en het systeem onbewust bestaande generaliseringen voortzet of zelfs versterkt, zonder dat daarvoor een rechtvaardiging bestaat.[624]
- Op strafrechtelijk terrein kan het in hoofdstuk I besproken Criminaliteits Anticipatie Systeem (CAS) leiden tot intensivering van het toezicht in wijken waarin etnische minderheden oververtegenwoordigd zijn. Dit kan resulteren in algoritmische etnische profilering. Ook toepassing van het iColumbo-zoeksysteem kan eenvoudig tot discriminatie leiden. Deze politiële Big Data-toepassing sluit niet uit dat zoekslagen zich

621 Citron & Pasquale 2014, p. 14. Zie ook over 'credit scoring': Hurley & Adebyo 2016, p. 148.
622 Zie hierover o.a. Squires 2003.
623 Zie infra hoofdstuk I, para. 2.3 en specifiek over, bijvoorbeeld, vacatureadvertenties Dalenberg 2017.
624 Zie infra hoofdstuk I, para. 2.3.2 en Niklas, Sztanderska & Szymielewicz 2015, p. 21.

richten op geaardheid, etniciteit of geloofsovertuiging.[625] Op zichzelf kan dit aanvaardbaar zijn, maar opnieuw vraagt dit wel om het bewust nadenken over de aanwezigheid van een objectieve en redelijke rechtvaardiging.

III.2.3 Oorzaken en effecten van algoritmische discriminatie

De hiervoor omschreven voorbeelden van discriminatie door algoritmes kennen hoofdzakelijk twee oorzaken: (1) een of meer *biases* in de data of (2) een of meer *biases* in het algoritme.[626] Deze oorzaken, ook wel aangeduid als 'sluipwegen' die bewust of onbewust en direct of indirect kunnen leiden tot discriminatie,[627] worden hieronder besproken. Daarna wordt afzonderlijk ingegaan op het maskeren van algoritimische discriminatie, en op de effecten van algoritmische *biases*.

III.2.3.1 Bias in de data

'An algorithm is only as good as the data it works with'. Een algoritme kan worden gekoppeld aan een dataset die *biases* bevat of vertrekt vanuit al te brede stereotypen of vooroordelen. Datasets kunnen daardoor gegevens bevatten die niet in een algoritmisch model mogen worden opgenomen, omdat het verdachte kenmerken betreft of omdat er een correlatie bestaat tussen ogenschijnlijk neutrale gegevens en de gegevens over verdachte kenmerken, zonder dat er een rechtvaardiging bestaat voor het in besluitvorming betrekken van dit soort gegevens.[628] Het opnemen van gegevens over religie of seksuele gerichtheid stelt een algoritme bijvoorbeeld in staat om verborgen verbanden te vinden tussen deze persoonskenmerken en bijvoorbeeld kredietwaardigheid, terwijl het vanuit het perspectief van het discriminatieverbod maar zeer de vraag is of het redelijk is dat deze kenmerken bij het verstrekken van leningen een rol spelen.[629] De *output* van de algoritmische analyse zal vervolgens kunnen resulteren in een verdachte ongelijke behandeling of in discriminatie. De uitdrukking 'garbage in, garbage out' wordt in dit kader veelvuldig gebruikt.[630] Als data verborgen vooroordelen bevat, kan het algoritmisch proces eveneens eenvoudig worden samengevat: 'discrimination in, discrimination out.'

625 Zie hierover Brinkhoff 2016, p. 1406.
626 Zie White House 2016, p. 6-7 voor dit onderscheid.
627 De Hert, Lammerant & Blok 2017, p. 127.
628 De Hert, Lammerant & Blok 2017, p. 134.
629 Het wordt algemeen aangenomen dat het verwijderen van dergelijke gegevens uit datasets kan voorkomen dat wordt gedifferentieerd aan de hand van verboden gronden. Recent onderzoek laat echter zien dat het opnemen van deze gronden juist noodzakelijk kan zijn om discriminatie te voorkomen; zie Žliobaitė & Custers 2016.
630 Voor beide uitdrukkingen zie Barocas & Selbst 2016, respectievelijk p. 671 en 683-684.

Nog problematischer kan de situatie worden wanneer gebruik wordt gemaakt van *training data* bij voorspellende analyses.[631] Als de training data een *bias* bevatten, zal het algoritme dit immers reproduceren in de data-analyse en leert het algoritme een discriminatoire benadering aan. Vaak gebeurt dit onbewust en bijna ongemerkt. Zo kan het voorkomen dat de gegevens van een bepaalde groep over- of ondervertegenwoordigd zijn in een dataset. In dat geval kan het resultaat van data-analyse uitvallen in het voor- of nadeel van deze groep. Als de politie bijvoorbeeld intensief surveilleert in buurten waarin vooral etnische minderheden wonen (ook al is daar geen verhoogd risico voor bijvoorbeeld inbraken of berovingen geconstateerd), raken de politiedatabases onbewust gevuld met informatie over deze minderheden. Wanneer risicoprofielen worden opgesteld in het kader van misdaadpreventie, kunnen deze minderheden worden aangemerkt als risicoverhogend. Deze profielen kunnen vervolgens worden verwerkt, bijvoorbeeld in de *heatmaps* van het Criminaliteits Anticipatie Systeem, waardoor er (nog) meer gesurveilleerd wordt in de betreffende buurten en leden van minderheden mogelijk nog vaker en scherper in de gaten worden gehouden. Zo leidt een *bias* in gegevensverzameling tot een *selffulfilling prophecy* met nadelige gevolgen voor bepaalde groepen, zonder dat daar een goede en objectieve rechtvaardiging voor bestaat.[632] Op een vergelijkbare manier kunnen veiligheidschecks op vliegvelden of tijdens verkeerscontroles resulteren in discriminatoire algoritmische besluitvorming als ze zich op voorhand al vooral richten op etnische of religieuze minderheden.[633]

Tot slot is relevant dat de data waarmee een algoritme worden getraind reeds geclassificeerd kunnen zijn. Ook deze classificatie (ook wel 'labeling') kan ongemerkt vooroordelen bevatten. Barocas en Selbst schrijven dienaangaande: 'The unavoidably subjective labeling of examples will skew the resulting findings such that any decisions taken on the basis of those findings will characterize all future cases along the same lines.'[634] Een voorbeeld is een algoritme dat de geschiktheid van sollicitanten voor een vacature bepaalt. Dit algoritme is getraind met behulp van gegevens over eerdere sollicitanten bij het bedrijf die als 'succesvol' zijn geclassificeerd. Daarbij wordt 'succesvol' gedefinieerd als 'eerder snel doorgestroomd naar hogere functies'. Die definitie kan inherent een indirecte discriminatie opleveren, bijvoorbeeld wanneer gedurende een langere periode vrouwen er door maatschappelijke en culturele oorzaken maar beperkt in slagen om door te stromen naar hogere functies (het bekende 'glazen plafond'). In dat geval zullen slechts weinig vrouwen als 'succesvol' worden aangemerkt in de *training data*. Het probleem van indirecte discriminatie wordt vervolgens nog versterkt doordat het algoritme de afwezigheid van vrouwen

631 *Infra*, hoofdstuk I, para. 2.2.
632 Custers 2017, p. 33.
633 Calders & Žliobaitė 2012, p.47.
634 Barocas & Selbst 2016, p. 681.

in hogere functies zal herkennen als teken van 'niet succesvol zijn' en het die kennis zal inzetten ten behoeve van het voorspellen van de slaagkans van sollicitanten.[635] Als een personeelsmanager dan besluit op basis van het algoritme ongeschikt geachte sollicitanten niet uit te nodigen op gesprek, zullen maar weinig vrouwelijke kandidaten uit het ogenschijnlijk 'objectieve' voorspellingssysteem voortvloeien. Een maatschappelijk ontstane ongelijkheid wordt op die manier in stand gehouden en zelfs versterkt door algoritmische besluitvorming.

III.2.3.2 Bias in het algoritme

Een *bias* kan ook, bewust of onbewust, worden vastgelegd in het ontwerp van het algoritme dat wordt gebruikt voor data-analyse. In de woorden van Pasquale en Citron:

> 'Software engineers (…) define the parameters of data-mining analyses; they create the clusters, links, and decision trees applied; they generate the predictive models applied. The biases and values of system developers and software programmers are embedded into each and every step of development.'[636]

Een programmeur bepaalt waartoe een algoritme wordt ingezet. De *outcome* van het algoritme, ook wel aangeduid als doelvariabele, kan bijvoorbeeld worden uitgedrukt in een risicoscore of in een oordeel over kredietwaardigheid. Mogelijke oorzaken van discriminatie doen reeds in deze fase hun intrede, omdat de keuze voor een bepaalde doelvariabele noodzakelijkerwijs subjectief is en specifieke groepen mensen kan benadelen. Dit kan opnieuw worden geïllustreerd aan de hand van een algoritme dat wordt ingezet voor het aannemen van nieuwe werknemers. Als dit algoritme zich richt op het voorspellen van het personeelsverloop als doelvariabele kan discriminatie optreden als blijkt dat vroegtijdig vertrek bij mensen met een chronische ziekte veel vaker voorkomt dan bij gezonde mensen. Hoewel het ogenschijnlijk redelijk en rationeel is om als bedrijf alleen personen aan te nemen die volgens een algoritme voor langere tijd aan het bedrijf verbonden blijven, kan het formuleren van een doelvariabele gericht op personeelsverloop mogelijk discriminatoir uitwerken in het licht van het verbod discriminatie jegens mensen met een chronische ziekte.[637]

Daarnaast richten datamining-algoritmes zich op het vinden van correlaties die relevant zijn voor het bepalen van een doelvariabele. Hiervoor is reeds gewezen op het risico van de aanwezigheid van data in de dataset die direct of indirect iets zeggen over de verboden

635 Calders & Žliobaitė 2012, p. 50 en voor een soortgelijk voorbeeld Barocas & Selbst 2016, p. 682.
636 Pasquale & Citron 2014, p. 14.
637 Vgl. Barocas & Selbst 2016, p. 677-680 en zie de Wet gelijke behandeling op grond van handicap en chronische ziekte (WGBH/CZ), ook kort beschreven in par. 2 van hoofdstuk II.

gronden van onderscheid. Deze informatie kan door het algoritme worden gebruikt als 'voorspellende variabele' bij het bepalen van de doelvariabele. Algoritmes kunnen in hun zoektocht naar correlaties dan ook discriminerende verbanden ontdekken.[638]

III.2.3.3 Het maskeren van discriminatie

De hiervoor omschreven oorzaken van discriminatie kunnen een onbedoeld neveneffect zijn van algoritmische besluitvorming, maar 'any form of discrimination that happens unintentionally can also be orchestrated inentionally.'[639] Bij dataverzameling kunnen opzettelijk data van bepaalde etnische groepen worden meegenomen, doelvariabelen kunnen zo geformuleerd worden dat deze welhaast zeker tot discriminatie van vrouwen leiden en algoritmes kunnen bewust met behulp van discriminatoire *training data* worden getraind. Ook als informatie over de verboden gronden van discriminatie niet als zodanig in een dataset zichtbaar is, wil dat bovendien nog niet zeggen dat algoritmes er geen gebruik van kunnen maken. Klassiek geldt in het discriminatierecht al het probleem dat een besluitvormer soms welbewust niet gebruik maakt van het eigenlijke verdachte kenmerk (bijvoorbeeld nationale afkomst), maar van een daarop sterk lijkend, gemakkelijker te rechtvaardigen kenmerk (bijvoorbeeld het als 'native speaker' spreken van de landstaal). Het is dan erg lastig om eventuele discriminatoire bedoelingen te achterhalen.[640] Dit probleem doet zich bij algoritme-gedreven besluitvorming nog sterker voor. Een belangrijk fenomeen dat hierbij aandacht verdient is *masking*, ofwel het maskeren van bepaalde kenmerken.[641] Als algoritmes met discriminatoire bedoelingen worden ingezet kan dit worden verborgen door ogenschijnlijk triviale, neutrale gegevens te gebruiken als indicatoren voor verdachte eigenschappen. Via datamining kan zelfs bewust worden gezocht naar verafgelegen, ogenschijnlijk neutrale indicatoren, die uiteindelijk iets zeggen over ras, politieke voorkeur, geslacht of leeftijd.[642] Door de complexiteit en ondoorzichtigheid van algoritmes is dit moeilijk te ontdekken, ook al omdat niet altijd duidelijk is welke verbanden de uitkomst van de analyse bepalen.[643] Algoritmisch geconstateerde discriminerende verbanden kunnen op die manier bepalend zijn voor belangrijke beslissingen, zonder dat adequate controle mogelijk is.

III.2.3.4 De effecten van algoritmische biases

De uiteindelijke effecten van *biases* in data-analyse hangen af van de mate waarin besluiten (al dan niet automatisch) gegrond worden op de uitkomsten van deze data-analyse. Als

638 De Hert, Lammerant & Blok 2017, p. 128-129.
639 Barocas & Selbst 2016, p. 692.
640 Zie hoofdstuk II, par. 2.
641 Zie daarover Custers 2013, p. 9-10.
642 Zie voor wat betreft het gevaar van datamining naar politieke voorkeur ook de probleemverkenning van de Staatscommissie parlementair stelsel 2017, p. 49 e.v.
643 De Hert, Lammerant & Blok 2017, p. 128-129.

de uitkomsten van analyse het te nemen besluit bepalen, dringt een *bias* in de data-analyse direct door in de levens van mensen. Maar ook als een algoritmisch voorbereide beslissing officieel door mensen wordt genomen, dreigt het gevaar dat *biases* het uiteindelijk te nemen besluit beïnvloeden. Het ontbreekt mensen immers veelal aan de kennis en het (technologische) inzicht om discriminatie door algoritmes te herkennen.[644] Dit kan ingrijpende gevolgen hebben, zoals bij besluitvorming op basis van aanwijzingen door algoritmes in het veiligheidsdomein, bij sollicitatieprocedures, bij kredietverlening of bij het bepalen van de hoogte van verzekeringspremies. De in paragraaf III.2.2 gegeven voorbeelden laten dit al zien.

III.2.4 Grondrechtelijke aandachtspunten

Zoals eerder gezegd voert het te ver om in dit onderzoek in te gaan op alle mogelijke manieren waarop algoritmische besluitvorming in een Big Data-context kan leiden tot directe of indirecte discriminatie en op de mate waarin de huidige grondrechtencodificaties een antwoord bieden op de hierboven beschreven risico's van discriminatie en ongerechtvaardigde ongelijke behandeling. Niettemin kunnen enkele algemene opmerkingen worden gemaakt over potentiële grondrechtelijke aandachtspunten in dit verband.

Allereerst is van belang dat de codificaties van het gelijkheidsbeginsel en het discriminatieverbod niet van toepassing zijn als de verzameling en analyse van data niet leidt tot benadeling.[645] Dat betekent bijvoorbeeld dat een verzekeringsbedrijf gegevens over geslacht of etniciteit kan gebruiken voor het vaststellen van het verzekeringsrisico op bedrijfsniveau of om gemiddelde verzekeringspremies te berekenen. De regels inzake gelijke behandeling zijn pas van toepassing als sprake is van een concreet nadeel voor een groep of persoon ten opzichte van een andere groep of persoon zijn.[646] Door de ondoorzichtigheid en complexiteit van algoritmes zal voor veel mensen echter onduidelijk of zelfs onzichtbaar zijn of sprake is van een concrete benadeling, waardoor zij niet gemakkelijk zullen kunnen opkomen tegen een aantasting van hun recht op non-discriminatie. Met betrekking tot kredietscores stellen Pasquale en Citron bijvoorbeeld vast dat 'credit bureaus may be laundering discrimination into black boxed scores, which are immune from scrutiny.'[647] De ondoorzichtigheid van algoritmes beïnvloedt de mate waarin algoritmische discriminatie kan worden ontdekt en gecontroleerd. Een juridisch en grondrechtelijk relevant

644 Dit werd reeds kort aangestipt in hoofdstuk I, par. 5.1 en 5.2.
645 De Hert, Lammerant & Blok 2017, p. 125.
646 Zie nader hoofdstuk II, par. 2.1.1.
647 Citron & Pasquale 2014, p. 14.

probleem is dan ook vooral gelegen in de sfeer van zichtbaarheid en bewijs van ongelijke behandeling.

Met name het intentioneel 'maskeren' van de werking van algoritmes is moeilijk aantoonbaar. Dit is des te problematischer, omdat er wel juridische betekenis uitgaat van de vraag of sprake is van een welbewust op een (al dan niet gemaskeerde) verdachte grond gebaseerd onderscheid en een onbewuste ongelijke behandeling. Bij intentionele discriminatie kan immers sprake zijn van strafbaar gedrag in de zin van de artikelen 137g en 429quater van het Wetboek van Strafrecht. Opzettelijke discriminatie valt onder artikel 137g Sr en wordt zwaarder bestraft dan strafbare discriminatie als omschreven in artikel 429quater Sr, omdat in deze laatste bepaling het opzetvereiste ontbreekt. Het maakt daarmee strafrechtelijk gezien uit of discriminatoire elementen bewust of onbewust in een dataset of algoritme zijn opgenomen.

Ook verder stelt algoritme-gedreven besluitvorming de nodige uitdagingen als het gaat om het gelijkebehandelingsrecht. In paragraaf III.2.1 is al opgemerkt dat, zodra onderscheid wordt gemaakt op individueel niveau, de vraag rijst welke regime de relevante rechtsverhoudingen bepaalt. Of specifieke wetgeving van toepassing is, hangt af van de gronden waarop onderscheid wordt gemaakt en het gebied waarop dit gebeurt. Big Data-toepassingen worden bijvoorbeeld veel gebruikt bij het verstrekken van verzekeringen en leningen. Voor zover sprake is van onderscheid op grond van geslacht geldt hiervoor de relevante EU-regelgeving,[648] maar dat is niet het geval als mensen blijken te worden benadeeld op grond van hun godsdienst of sexuele gerichtheid. De EU-richtlijn die ongelijke behandeling op deze gronden verbiedt heeft immers alleen betrekking op het terrein van de arbeid.[649] De AWGB is vanwege zijn toepasselijkheid op het aanbieden van goederen en diensten dan weer wel relevant, net als uiteraard algemene bepalingen als die van art. 1 Grondwet, art. 14 EVRM en art. 26 IVBPR. Hoewel die bepalingen geen heel concrete normen geven voor bepaalde typen van ongelijke behandeling gebaseerd op bepaalde gronden, kan vooral uit de rechtspraak vaak specifieker worden afgeleid of een bepaald onderscheid aanvaardbaar is. Deze algemene bepalingen kunnen dan ook dienen als 'vangnet' om een door algoritmetoepassingen ontstane discriminatie aan te pakken, ook als die niet concreet binnen het bereik van een specifiekere wet valt.

Het kwalificatieprobleem is niettemin relevant, omdat specifieke wetgeving, zoals in paragraaf II.2.2 besproken, meestal een hoger beschermingsniveau biedt bij directe discri-

648 Zie in het bijzonder HvJ 1 maart 2011, zaak C-236/09, ECLI:EU:C:2011:100 (*Test-Achats*), *EHRC* 2011/64 m.nt. Y. Thiery, *NJ* 2011/120 m.nt. M.R. Mok.

649 Zie hoofdstuk II, par. 2.2.

minatie. Dit is in die zin lastig dat het bij de toepassing van algoritmes bij Big Data-analyses 'altijd gaat om een veelheid aan factoren'.[650] In de eerste plaats maakt dit het voor een slachtoffer lastig om aan te tonen dat een algoritmisch besluit rechtstreeks is gebaseerd op een verboden grond. Als geen inzicht wordt geboden in de dataset of de werking van een algoritme, zal het slachtoffer moeten aantonen dat een beslissing anders uitpakt voor iemand, die zich, op de verboden grond na, in exact dezelfde situatie bevindt als het slachtoffer. In de tweede plaats is het bijzonder moeilijk om directe discriminatie aan te tonen als verdachte gronden niet herkenbaar zijn, maar gewerkt wordt met ogenschijnlijk neutrale indicatoren die iets zeggen over bijvoorbeeld ras of godsdienst. In de derde plaats kan het direct betrekken van een bepaalde grond verwaterd raken als er nog veel meer variabelen worden betrokken in de besluitvorming, wat bij algoritme-gedreven besluitvorming bijna stelselmatig het geval is. Ook daardoor kan het moeilijk zijn om een daadwerkelijk directe discriminatie aan te tonen en te profiteren van de rechtsbescherming die bijzondere gelijkebehandelingswetgeving op dit punt biedt.

In veel gevallen kan wel het leerstuk van indirecte discriminatie uitkomst bieden. Een individu dat zich benadeeld voelt door een door algoritme-gedreven besluit, kan bijvoorbeeld laten zien dat bepaalde algoritme-gedreven besluiten leiden tot disproportioneel nadelige resultaten voor een bepaalde groep. Zo kan iemand betogen dat een algoritme dat wordt gebruikt bij werving en selectie disproportioneel benadelend uitpakt voor vrouwen door te laten zien dat in een reeks van gevallen vrouwen stelselmatig worden afgewezen of niet op gesprek worden uitgenodigd. In dat geval moet de werkgever aantonen dat het redelijk is om zijn besluiten op basis van het algoritme te nemen. In deze gevallen zal het voor de betrokkene niet direct nodig zijn om de precieze bron van de discriminatie te lokaliseren (bijvoorbeeld de selectie van de dataset, het algoritme, of het lerende effect van een algoritme), maar kan hij (of zij) zich louter richten op de effecten ervan.

Hoewel het concept van indirecte discriminatie hierbij dus een oplossing kan bieden, is die zeker niet ideaal. Allereerst zijn er niet de voordelen die de specifiekere wetgeving over directe discriminatie heeft in termen van scherpe rechtvaardigheidseisen, rechtszekerheid, houvast voor werkgevers en aanbieders van diensten en goederen, en toetsbaarheid voor de rechter. Daarnaast werkt de constructie via indirecte discriminatie alleen goed wanneer er een voldoende groot aantal gevallen is om een discriminerend effecten te kunnen laten zien. De bewijslast die rust op de betrokkene is daarmee aanzienlijk.

Verder is in hoofdstuk II toegelicht dat het voor het gelijkebehandelingsrecht niet uitmaakt of een gediscrimineerde persoon daadwerkelijk beschikt over de kenmerken op grond

650 De Hert, Lammerant & Blok 2017, p. 125.

waarvan hij of zij nadelig is behandeld.[651] Discriminatie op grond van 'vermeende' persoonskenmerken is ook verboden, net als discriminatie op grond van het associëren van een persoon met de persoonskenmerken van iemand anders.[652] Ook deze leerstukken zijn relevant voor het gebruik van Big Data-analyses. Ze impliceren bijvoorbeeld dat wanneer Facebook vacatureadvertenties afstemt op de vermeende homoseksualiteit van een gebruiker, sprake kan zijn van discriminatie, ook wanneer deze gebruiker zelf geen homoseksueel is. Hetzelfde geldt als een algoritme aandacht blijkt te besteden aan het feit dat een sollicitant misschien niet zelf chronisch ziek is, maar wel zorg draagt voor iemand anders met een chronische ziekte.[653]

III.3 Vrijheidsrechten

III.3.1 Inleiding

Hiervoor is ingegaan op de effecten van nieuwe, algoritme-gedreven technologieën voor de privacy en voor gelijkheidsrechten. Belangrijke effecten zijn er daarnaast voor de in hoofdstuk II onderscheiden andere vrijheidsrechten: de vrijheid van meningsuiting, de vrijheid van godsdienst, de demonstratievrijheid, de verenigingsvrijheid en het hieraan verwante kiesrecht. Hoewel deze grondrechten traditioneel vooral beschermen tegen inmenging door de staat, is duidelijk dat hieraan ook een zekere betekenis toekomt in verhoudingen tussen private spelers. Dit is van belang, nu blijkt dat onder meer Big Data-analyses door bedrijven een belangrijke rol kunnen spelen als het gaat om de uitoefening van de in hoofdstuk II beschreven vrijheidsrechten. In dit verband is ook van belang dat in hoofdstuk II is gebleken dat de staat zich niet alleen heeft te onthouden van onredelijke beperkingen van deze vrijheden, maar dat er ook positieve verplichtingen bestaan om ze actief te beschermen – ook tegen bedrijven of andere private actoren.

In deze paragraaf wordt nader ingegaan op de impact van nieuwe technologieën voor de uitoefening en bescherming van deze grondrechten. Daarbij wordt grofweg dezelfde volgorde van bespreking gehanteerd als in hoofdstuk II. Vermeldenswaard is dat de vrijheid van godsdienst en levensovertuiging hier niet afzonderlijk wordt besproken. Voor zover het daarbij gaat om het 'forum internum', dus de gewetensvrijheid en het recht om een godsdienst te hebben (zonder die te uiten), is deze vrijheid al even aan de orde gekomen in paragraaf II.2. Voor zover het gaat om het 'forum externum' zijn er veel dwarsverbanden

651 HvJ 17 juli 2008, zaak C-303/06, ECLI:EU:C:2008:415 (*Coleman*), *EHRC* 2008/108 m.nt. A.C. Hendriks, *NJ* 2008/501 m.nt. M.R. Mok, TRA 2008 m.nt. Veldman. Zie hoofdstuk II, par. 2.2

652 Zie nader hoofdstuk II.

653 Zie het in hoofdstuk II, par. 2.1.3 gegeven voorbeeld.

met de vrijheid van meningsuiting (bijvoorbeeld waar het gaat om het uiten van een godsdienst door het dragen van religieuze kleding of online religieuze uitingen), de vrijheid van vergadering, demonstratie of betoging (bijvoorbeeld waar het gaat om religieuze samenkomsten) of de vrijheid van vereniging (bijvoorbeeld waar het gaat om de erkenning of ontbinding van geloofsgemeenschappen). Uiteraard zijn er verschillen in regulering, zoals besproken in hoofdstuk II, maar deze verschillen zijn niet bijzonder relevant voor het onderhavige hoofdstuk.

III.3.2 Vrijheid van meningsuiting en vrijheid om informatie te ontvangen

Algoritmes hebben een potentieel grote impact op de vrijheid van meningsuiting in de digitale samenleving. Hieronder wordt ingegaan op een drietal belangrijke knelpunten die in dit kader van belang zijn: (1) aantasting van de pluriformiteit en diversiteit van informatie en het ontstaan van 'filterbubbels', (2) de mogelijkheden tot algoritmische censuur van digitale meningsuiting en (3) het *chilling effect* dat op kan treden door het Internet of Things (IoT) en de inzet van algoritmes in een Big Data-context. Daaraan voorafgaand wordt echter eerst een positief punt belicht, namelijk de toename van toegang tot informatie en van mogelijkheden om informatie te openbare en te verspreiden.

III.3.2.1 Vrijheid van meningsuiting en diversificatie van het media-aanbod

Lange tijd waren het vooral grote mediaconglomeraten die bepaalden welke informatie tot mensen kwam. De nieuwsvoorziening was in handen van kranten, dagbladen, radiostations en tv-zenders. Het Internet wordt gezien als een motor van pluralisme in informatievoorziening. In het digitale tijdperk hebben burgers idealiter toegang tot een grote hoeveelheid aan bronnen en standpunten en beschikken zij tevens over de mogelijkheid om zichzelf online vrijelijk te uiten.[654] Digitale meningsuiting vindt vandaag de dag grotendeels plaats door middel van een private infrastructuur bestaande uit grote sociale media netwerken en invloedrijke zoekmachines. Bedrijven als Facebook, Google, YouTube en Twitter zijn niet primair zelf verantwoordelijk voor het produceren van 'content', maar richten zich op het verspreiden van informatie, nieuws, opinies en kennis geproduceerd door burgers zelf. Google's PageRank-algoritme verwerkt ruim 3,5 miljard zoekopdrachten per dag en uit recent onderzoek blijkt dat 31% van de Nederlanders nieuws vindt via sociale media.[655] De algoritmes die door deze bedrijven worden gebruikt, zijn verworden

654 Zie in dit kader de Mededeling van de Commissie aan het Europees Parlement, de Raad, het Europees Economisch en Sociaal Comité en het Comité van de Regio's, *Een Digitale Agenda voor Europa*, Brussel 19 mei 2010, COM(2010)245, p. 34.

655 Zie respectievelijk http://www.internetlivestats.com/google-search-statistics/ (geraadpleegd op 22 januari 2018) en Newman e.a. 2016, p. 92.

tot 'poortwachters' van vrije meningsuiting en informatievoorziening.[656] Hiermee zijn het niet langer primair de 'choices, methods and subjectivities' van traditionele mediabedrijven, maar die van algoritmes die bepalen welke informatie burgers bereikt.[657]

De hierboven weergegeven ontwikkelingen raken nauw aan de vrijheid van meningsuiting. Net als traditionele media moeten nieuwe intermediairs, zoals bedrijven die internetfora, zoekmachines, websites en sociale media beheren, de vrijheid hebben om naar eigen inzicht gedachten, gevoelens, informatie en feiten te delen.[658] Het ligt vanuit de rationale van de vrijheid van meningsuiting in de rede dat ook activiteiten als het vindbaar maken, prioriteren en filteren van informatie kunnen worden gerekend tot het recht op vrijheid van meningsuiting van de rechtspersonen die eigenaar zijn van zoekmachines en sociale media.[659] Of de nieuwe intermediairs deze bescherming ook altijd al krijgen, is overigens niet altijd duidelijk.[660]

Vanuit het perspectief van de vrijheid van meningsuiting is het verder een groot goed dat mensen door de nieuwe intermediairs zoveel middelen ter beschikking staan om hun gedachten, gevoelens en overtuigingen onder de aandacht te brengen. Sociale media hebben in de moderne democratische samenleving een belangrijke mobilisatie- en emancipatiefunctie – ze kunnen een belangrijke rol spelen bij het uitwisselen van meningen, opvattingen en inlichtingen of het organiseren van demonstraties (zie ook hierna, paragraaf III.3.3).[661] Daarnaast kunnen Big Data leiden tot maatschappelijk gezien belangrijke onthullingen, zoals de voorbeelden van klokkenluiders Assange en Snowden hebben laten zien, die aanvankelijk niet mogelijk waren.[662] Het feit dat tegenwoordig iedereen journalistieke content kan maken en kan verspreiden, maakt ook dat de media sterk zijn gedemocratiseerd en gediversificeerd, wat op zichzelf tot een groter en mogelijk meer onafhankelijk informatieaanbod kan leiden.[663]

III.3.2.2 Pluriformiteit en onafhankelijkheid van informatie

Vindbaarheid van informatie

Het Internet heeft gezorgd voor een brede beschikbaarheid van informatie en ideeën. Ook nieuwe intermediairs, zoals sociale media en zoekmachines, zijn steeds meer een essentiële

656 Over 'digital intermediaries' als 'gatekeepers' zie o.a. Vīķe-Freiberga 2013, p. 27.
657 Gillespie 2014, p. 191.
658 In deze trant Special Rapporteur on Freedom of Opinion and Expression 2016, p. 15.
659 Zie ook hoofdstuk II, par.3.2.1.
660 AIV 2014, p. 29; zie ook de voorbeelden van verantwoordelijkheid van webforumbeheerders besproken in hoofdstuk II, par. 3.2.3.
661 AIV 2014, p. 30; AIV 2017, p. 29.
662 AIV 2014, p. 30.
663 AIV 2017, p. 29.

schakel in het verschaffen van toegang tot informatie.[664] Zoals hiervoor aangegeven, heeft dit geleid tot een waardevolle diversificatie van het media- en informatieaanbod. Vanuit het perspectief van het recht om informatie te ontvangen is ook dit als waardevol te beschouwen.[665] Tegelijkertijd bestaan er risico's voor de onafhankelijkheid en pluriformiteit van de media, terwijl ook dat vanuit het perspectief van vrijheid van meningsuiting belangrijke waarden zijn.[666]

Een eerste knelpunt is gelegen in de online vindbaarheid van de informatie en ideeën.[667] De belangrijke positie van zoekmachines als Google, Yahoo! en Bing en sociale media als Facebook, Twitter en YouTube roept in dit kader grondrechtelijke vragen op. In paragraaf I.2.3.2, is gewezen op het gebruik van algoritmes die zoekresultaten prioriteren. Deze algoritmische prioritering bepaalt welke informatie we lezen, naar wie we luisteren en welke ideeën gehoord worden. Dergelijke prioritering is onvermijdelijk. Gelijke vindbaarheid van alle informatie is ondoenlijk en het is de taak van zoekmachines en sociale media om bronnen te rangschikken en gebruikers in staat te stellen relevante informatie te vinden. De centrale grondrechtelijke vraag is welke standaarden door algoritmes worden gebruikt om informatie te prioriteren en of pluriformiteit en toegankelijkheid van informatie hiermee voldoende gewaarborgd wordt.

De term 'search engine bias' is in dit verband bijzonder relevant. Deze term refereert aan de vele factoren die bepalen hoe zoekresultaten geprioriteerd en gemanipuleerd (kunnen) worden. Pasquale en Oren onderscheiden hierbij 'bias in the strong universal sense' en 'highly specific bias'.[668] 'Bias in the strong universal sense' ziet op algoritmische criteria die universeel gelden en die een grote hoeveelheid aan websites filteren en prioriteren. Dergelijke criteria geven, bedoeld of niet, voorrang aan de ene bron boven de andere. Deze vorm van prioritering begint reeds bij de selectie van webpagina's die vindbaar zijn via zoekmachines. Niet alle websites zijn namelijk geïndexeerd, bijvoorbeeld omdat Google's algoritme deze niet nuttig acht voor gebruikers, waardoor ze niet in de zoekresultaten terechtkomen.[669] Het blijkt bovendien dat de algoritmes van zoekmachines reeds populaire bronnen prefereren, Engelstalige sites rangschikken boven anderstalige bronnen en ernaar neigen om commerciële informatiebronnen een hoge positie te geven in zoekopdrachten.[670] De hoge prioritering van dergelijke pagina's gaat ten koste van de positie van andere websites en daarmee van de neutraliteit van de informatie die toegankelijk wordt gemaakt voor het publiek. Commerciële en politieke organisaties proberen de zoekresultaten van

664 AIV 2014, p. 29. Zie ook Special Rapporteur on Freedom of Opinion and Expression 2017.
665 Zie over dit recht nader hoofdstuk II, par. 3.2.1.
666 AIV 2017, p. 29; zie ook hoofdstuk II, par. 3.2.2.
667 Van Hoboken 2012, p. 282.
668 Pasquale & Oren 2008.
669 Bozdag 2013, p. 214-215.
670 Gillespie 2014, p. 177.

zoekmachines bovendien in hun voordeel te beïnvloeden.[671] Zoekmachineoptimalisatie ('Search Engine Optimization') is door dit alles inmiddels een belangrijke industrie, maar deze leidt niet altijd tot objectiviteit en neutraliteit van de aangeboden informatie. De financiële middelen van de organisaties achter websites kunnen een belangrijke rol spelen in de prioritering van zoekresultaten.[672] Zo is klimaatverandering het onderwerp geworden van een online strijd tussen klimaatsceptici en klimaatactivisten met Google als strijdveld. De New York Times schreef hierover: 'The climate denial ads on Google come amid a wider effort — backed by wealthy conservatives, fossil fuel companies and right-wing think tanks — to discredit the prevailing science on global warming and to prevent action.'[673] Zoekmachines zijn ontvankelijk voor commerciële invloeden. Zij zijn immers private bedrijven die voor hun winst grotendeels afhankelijk zijn van marketingstrategieën van financieel daadkrachtige actoren.

Naast deze 'bias in the strong universal sense' is er een 'highly specific bias' zichtbaar in de informatievoorziening bij gebruik van nieuwe technologieën. Deze categorie van 'bias' betreft gevallen waarin specifieke informatie een lagere (of hogere) ranking wordt toebedeeld en daardoor anders (minder goed of beter) wordt gepresenteerd. Zo spande de website Search King een procedure aan tegen Google nadat de site plotseling aanzienlijk was gedaald in Google's weergave van zoekresultaten. In de procedure liet Google de mogelijkheid open dat dit het gevolg was van het 'targeten' van de betreffende website.[674] Ook online-mediaplatforms kunnen specifieke bronnen algoritmisch of handmatig 'blacklisten'.[675] In het verlengde hiervan ligt het algoritmisch 'degraderen' van bepaalde video's of berichten. YouTube kan bijvoorbeeld weigeren suggestieve video's opnemen in 'most-watched' lijsten of op de homepage van gebruikers. Ook kan een algoritme bepaalde gevoelige tweets eenvoudigweg niet als 'trending' aanmerken.[676]

Het is de vraag in hoeverre pluriformiteit en objectiviteit van informatie een belangrijk criterium is voor de algoritmes die worden gebruikt voor filtering en prioritering.[677] Deze vormen van 'bias' en manipulatie kunnen ertoe leiden dat informatie niet neutraal en objectief wordt gepresenteerd, dat de stem van zwakkere partijen of minderheidsgroepen niet wordt gehoord, of dat onwelgevallige bronnen niet langer niet langer zichtbaar zijn. In de hiervoor genoemde gevallen gaat het daarbij steeds om het bieden van toegang van

671 AIV 2017, p. 29.
672 Van Hoboken 2012, p. 296 en 303-316.
673 New York Times, 'How Climate Change Deniers Rise to the Top in Google Searches', 29 December 2017, via: https://www.nytimes.com/2017/12/29/climate/google-search-climate-change.html (laatst geraadpleegd 18 februari 2018).
674 Zie over de zaak en Google's redenering in deze Grimmelmann, 2009, p. 945-947.
675 Bozdag 2013, p. 216-217.
676 Gillespie, p. 172.
677 Idem, p. 298.

informatie door private partijen, maar het is denkbaar dat overheidsorganen op dezelfde manier de toegang tot informatie beïnvloeden, bijvoorbeeld wanneer de staat nauwe banden heeft met bepaalde (media-)bedrijven of wanneer sprake is van betrokkenheid bij prioritering of 'blacklisting'.[678] De representativiteit en diversiteit van informatievoorziening kunnen daardoor sterk onder druk komen te staan.[679]

Filterbubbels

'Filterbubbels' vormen een specifieke manifestatie van het hiervoor aangeduide risico. Sunstein wees al in 2001 op het gevaar van 'information cocoons'.[680] Burgers zouden het Internet gebruiken om slechts kennis te nemen van hun welgevallige meningen.[681] Deze vorm van vrijwillige selectieve blootstelling kan worden aangeduid als 'zelfgeselecteerde personalisatie'.[682] In 2011 verscheen Pariser's bestseller *The Filter Bubble*, waarin hij een aanverwant probleem aankaart. In toenemende mate personaliseren websites, media-aanbieders, zoekmachines en sociale media de inhoud van hun platforms. Op basis van beschikbare gegevens over gebruikers wordt daarbij via algoritmes bepaald in welke informatie iemand waarschijnlijk is geïnteresseerd. Dit leidt tot het ontstaan van 'bellen' of 'bubbels' met 'a unique universe of information for each of us'.[683] De filterbubbel wordt ook wel gekarakteriseerd als 'vooraf geselecteerde personalisatie.'[684] Het is met name deze vorm van personalisatie die in dit hoofdstuk aandacht behoeft.

De grote hoeveelheid data die door en voor sociale media en andere actoren wordt verzameld stelt algoritmes in staat om informatievoorziening af te stemmen op de individuele gebruiker. In hoofdstuk I zijn reeds enkele voorbeelden vermeld van de werking van deze algoritmes. Associatie-algoritmes stellen bijvoorbeeld aanbieders van films, boeken of muziek in staat om producten aan te raden op basis van eerder keuzegedrag. Door middel van profilering kunnen sociale media zoals Facebook een uniek profiel van iedere gebruiker opstellen, waarop de inhoud van de 'Newsfeed' kan worden afgestemd. De zoekresultaten worden daarbij niet alleen geprioriteerd (zoals hierboven al beschreven), maar ook gepersonaliseerd. Op basis van eerder gebruik van de zoekmachine verschillen de zichtbare resultaten voor eenzelfde zoekopdracht dan voor iedere gebruikers.[685] In hun filterbubbel krijgen gebruikers daardoor enkel 'content' te zien die 'in hun straatje past.'[686] Opvattingen die niet gehuldigd worden door een gebruiker, komen daardoor niet in zijn

678 AIV 2017, p. 30; zie ook Morozov 2012.
679 Commissariaat voor de Media 2017, p. 46.
680 Sunstein 2001.
681 Idem.
682 Zuiderveen Borgesius e.a. 2016, p. 256.
683 Pariser 2011, p. 9.
684 Zuiderveen Borgesius e.a. 2016, p. 256.
685 Bozdag 2013, p. 209.
686 Commissariaat voor de Media 2017, p. 18.

of haar Newsfeed, en zoekresultaten of onderwerpen die hem of haar niet aanspreken worden niet getoond.

De filterbubbel kan leiden tot 'confirmation bias'. Het consumeren van informatie die onze opvattingen bevestigt is weliswaar eenvoudig en plezierig, maar verhindert genuanceerde meningsvorming. Daarvoor zijn contrasterende opinies nodig die onze aannames in twijfel trekken.[687] Doordat zij geen directe toegang meer hebben tot een pluriformiteit aan informatie, kunnen mensen ingekapseld raken in hun eigen opvattingen. Daardoor wordt ook de diversiteit en pluriformiteit in een democratische samenleving geraakt. Vooraf geselecteerde personalisatie blijkt polarisatie te versterken en deliberatie en consensusvorming te bemoeilijken.[688] Als algoritmes zo zijn ingericht dat ze alleen informatie laten zien waar gebruikers waarschijnlijk in geïnteresseerd zijn, verhindert dit gemakkelijke en brede kennisvergaring. Vooraf geprioriteerde en gepersonaliseerde informatie leidt bovendien tot fragmentatie van informatievoorziening, wat uiteindelijk het recht van burgers beperkt om vrijelijk informatie te ontvangen.

Het negatieve effect van de hierboven beschreven fenomenen op de vrijheid van meningsuiting en de informatievrijheid wordt nog versterkt doordat de kwaliteit van de uitkomst van een zoekopdracht kan verschillen per gebruiker. De keuze van een gebruiker voor een specifieke zoekmachine, zijn of haar talenkennis en de mogelijkheid om zoekopdrachten te formuleren en herformuleren hebben een aanzienlijke invloed op, bijvoorbeeld, de diversiteit van zoekresultaten.[689] Veel gebruikers van zoekmachines ontbreekt het aan de kennis en vaardigheden om te ontsnappen aan de nadelige effecten van door zoekmachines opgeworpen filterbubbels. Hetzelfde geldt voor nieuwsvoorziening via sociale media. Dit is des te gevoeliger omdat belangstelling in nieuws en politiek veelal samen blijkt te hangen met opleidingsniveau en sociaaleconomische achtergrond.[690] Daarmee is er een risico dat laagopgeleiden in mindere mate in staat zijn om te komen tot een brede blik op de maatschappij. Filterbubbels hebben zo dus ook een potentieel negatieve impact op de *gelijke toegang* tot pluriforme informatie.

De nadelige consequenties die filterbubbels kunnen hebben op de informatievoorziening en pluriformiteit zijn in de literatuur al vaak genoemd. Belangrijk is wel te vermelden dat veel claims (nog) niet empirisch zijn onderbouwd. Het is onduidelijk in welke mate vooraf geselecteerde personalisatie voorkomt, of filterbubbels daadwerkelijk bestaan en welk effect zij hebben op mensen en hun gedrag.[691] Dat neemt niet weg dat de potentiële invloed van

687 Bozdag 2013, p. 218.
688 Vīķe-Freiberga e.a. 2013, p. 27; Zuiderveen Borgesius e.a. 2016, p. 260.
689 Van Hoboken 2012, p. 301-302.
690 Zuiderveen Borgesius 2016, p. 260.
691 Idem.

filterbubbels groot is. Algoritmes, kunnen wanneer gecombineerd met grote hoeveelheden data over individuele burgers, een grote impact hebben op de vrijheid van meningsuiting van burgers.

III.3.2.3 Algoritmische censuur

Zoals hierboven beschreven heeft het prioriteren van informatiebronnen effecten voor de toegankelijkheid van informatie. Daarnaast kan het leiden tot een vorm van voorafgaande beperking van de vrijheid van meningsuiting. Sommige bronnen zullen als gevolg van dit proces wel beschikbaar, maar (extreem) lastig vindbaar zijn. Het algoritmisch verwijderen van bepaalde informatie van, bijvoorbeeld, sociale media platforms is van een andere grondrechtelijke orde. Classificatie-algoritmes zijn in staat om onwelgevallige, verdachte of gevaarlijke content te herkennen en niet te uploaden of automatisch te verwijderen.[692] Zowel bedrijven als de overheid kunnen dergelijke algoritmes voor dit doel gebruiken – voor algoritmische censuur dus.

Private censuur

YouTube, Facebook en Twitter hebben uitgebreide algemene voorwaarden en interne richtlijnen opgesteld om te bepalen welke content toegestaan is en welke berichten van gebruikers verwijderd worden.[693] Een brede categorie aan opinies en berichten kan worden verwijderd en content die in strijd is met interne voorwaarden en richtlijnen is niet per definitie strafbaar. Er zijn hoofdzakelijk drie manieren waarop deze bedrijven de content op hun platforms monitoren:[694]

1. Door middel van *ex ante*-controle kan, bijvoorbeeld, Facebook voorkomen dat content geplaatst wordt. Wanneer een gebruiker een video upload, verschijnt het bericht in beeld dat de video door Facebook wordt verwerkt en dat de gebruiker een bericht ontvangt zodra deze klaar is om te bekijken.[695] *Ex ante*-controle vindt plaats tussen het moment van uploaden en publicatie. In deze tussenliggende periode voert een algoritme een controle uit, veelal zonder menselijke betrokkenheid. Op deze wijze kan worden voorkomen dat strafbaar materiaal, zoals kinderporno, wordt gepubliceerd.
2. Bij proactieve *ex post*-controle gaat een platform, met behulp van algoritmes, op zoek naar onwenselijke content, waarna deze wordt verwijderd. Zo zijn sociale media zich in toenemende mate gaan toeleggen op het verwijderen van extremistisch, terroristisch en haatzaaiend materiaal.[696] Met behulp van zelflerende algoritmes willen onder andere

692 Vgl. het in paragraaf 2.2.2 aangehaalde voorbeeld van spamfilters.
693 Balkin 2017, p. 37.
694 Klonick 2018.
695 Facebook helpcentrum, 'Hoe plaats ik een video op Facebook?', https://nl-nl.facebook.com/help/166707406722029?helpref=about_content.
696 'Google en Facebook: harder tegen terreur en haatzaaien', *NRC Handelsblad*, via: https://www.nrc.nl/nieuws/2017/06/20/google-en-facebook-harder-tegen-terreur-en-haatzaaien-11173871-

Google en Facebook dergelijke video's en berichten sneller en nauwkeuriger opsporen en verwijderen.

3. Bij reactieve *ex post*-controle wordt mogelijk problematische content door andere gebruikers gesignaleerd en aan het platform doorgegeven. Veelal beoordelen menselijke moderatoren, al dan niet met behulp van algoritmes, of de content verwijderd moet worden.

Grote delen van het controleproces worden aldus uitgevoerd door slimme algoritmes. Deze worden ingezet voor de analyse van de grote hoeveelheid data die wordt gegenereerd op sociale media platforms.[697] Het EHRM heeft aanvaard dat dit soort private censuur plaatsvindt, als die noodzakelijk is om zwaarwegende algemene belangen te beschermen, zoals de eer en goede naam van derden.[698] Er bestaan echter belangrijke risico's voor de vrijheid van meningsuiting door de werking van dit soort algoritmes. Vaak zijn ze weliswaar in staat om strafbare en anderszins illegale content te verwijderen, maar op dit moment zijn algoritmes vaak onnauwkeurig zijn en daardoor kunnen ze fouten maken.[699] Dit kenmerk wordt versterkt doordat het lastig is om objectief te bepalen welk materiaal geldt als smadelijk, extremistisch, haatzaaiend of pornografisch. De foto van het naakte Vietnamese 'napalm-meisje' is een treffend voorbeeld. Nadat een gebruiker, een beroemde Noorse auteur, deze foto op Facebook had geplaatst werden de foto en de account van de gebruiker verwijderd, waarschijnlijk omdat deze in strijd was met interne richtlijnen omtrent de publicatie van naaktfoto's. Ook toen de hoofdredacteur van een krant en de Noorse premier de foto plaatsten, werden deze verwijderd, en hoogstwaarschijnlijk was dezelfde foto al duizenden keren eerder geplaatst en verwijderd.[700] Enige tijd later bood Facebook excuses aan en beloofde het bedrijf beterschap bij het detecteren van dergelijk materiaal.

Van belang is verder dat de grens tussen het aanvaardbare en het onaanvaardbare een dunne is. Met name kunstzinnige of grove, sterk opiniërende uitingen die aanschurken tegen het onaanvaardbare, zullen mogelijk al te snel worden verwijderd omdat ze in strijd zijn met de algemene voorwaarden of interne richtlijnen van platforms.[701] De vrijheid van meningsuiting beschermt echter juist ook uitingen die 'shock, offend or disturb'.[702] Voor-

a1563731 en 'Facebook Steps Up Efforts Against Terrorism', *Wall Street Journal*, via: https://www.wsj.com/articles/facebook-steps-up-efforts-against-terrorism-1455237595.

697 Vgl. Wagner 2017, p. 12.

698 Zie nader hoofdstuk II, par. 3.2.3.

699 Zie hoofdstuk I, par. 5.2.

700 Klonick 2017, p. 64-65.

701 Tushnet 2008, p. 1015-1016.

702 Zie hoofdstuk II, par. 3.

afgaande beperkingen van de vrijheid van meningsuitingen worden juist daarom ook altijd met grote terughoudendheid bekeken.[703]

'New School speech regulation' – indirecte publieke censuur

De rol van de overheid bij het reguleren van de vrijheid van meningsuiting verandert hoe dan ook doordat digitale informatievoorziening steeds meer via een private infrastructuur plaatsvindt. In aanvulling op het direct beperken van strafbare of anderszins onrechtmatige uitlatingen, richten overheden zich op de platforms waarop mensen hun mening uiten. Balkin duidt dit aan als '*New School' speech regulation*, waarbij overheden samenwerken met of dreigen met dwang richting Facebook, Google en andere bedrijven om content te verwijderen.[704] De recent in Duitsland aangenomen wet ter bestrijding van haatzaaien en *fake news* biedt een goed voorbeeld. Sociale media kunnen boetes opgelegd krijgen (oplopend tot 50 miljoen euro) wanneer zij illegale content niet (tijdig) van hun platform verwijderen.[705] Ook in Nederland is door het Centraal Planbureau het voorstel gedaan om een vergunningenstelsel voor platforms als Facebook en Youtube in te voeren. Er zouden onvoldoende prikkels zijn voor platformbedrijven om ongewenst gedrag van gebruikers tegen te gaan en het voorgestelde systeem zou noodzakelijk zijn om de aansprakelijkheid van de platforms te vergroten.[706] Deze manier van regulering kan leiden tot overmatige voorafgaande beperkingen door deze bedrijven, die weten dat zij aansprakelijk kunnen worden gesteld voor vermeende onrechtmatige uitingen op hun platforms. Zo hebben oproepen vanuit de Verenigde Staten en de Verenigde Naties een rol gespeeld bij de beslissing van YouTube en Facebook om vermeende terroristische content automatisch te gaan verwijderen.[707] Ook de EU is in dit verband voornemens strenge maatregelen te nemen.[708] Dit levert een door Balkin als volgt omschreven beeld op: 'In addition to private governance we must add the phenomenon of new school speech regulation. Above or beyond the digital governors, there are territorial governments, who constantly put pressure on digital governors to control their populations in certain ways.'[709] Dit alles maakt dat

703 Zie eveneens het in paragraaf II.3.3.1 besproken EHRM (GK) 16 juni 2015, nr. 64569/09 (*Delfi AS t. Estland*), ECLI:CE:ECHR:2015:0616JUD006456909, *EHRC* 2015/172 m.nt. B. van der Sloot, NJB 2015/1630, NJ 2016/457 m.nt. E.J. Dommering.

704 Balkin 2017, p. 4 en 27-36.

705 Zie https://www.theguardian.com/media/2017/jun/30/germany-approves-plans-to-fine-social-media-firms-up-to-50m (laatst geraadpleegd 22 februari 2018). Zie ten aanzien van de bestrijding van nepnieuws ook de werkzaamheden van de East StratCom Task Force van de EU.

706 Centraal Planbureau 2017 en in reactie de kamerbrief van de staatssecretaris van Economische Zaken en Klimaat, Beantwoording van verzoek tot reactie op de CPB Policy Brief 'Scientia potentia est: de makelaar van alles', 15 januari 2018.

707 Klonick 2017, p. 62.

708 Persbericht Europese Commissie, 'Een Europa dat beschermt: Europese Commissie intensiveert strijd tegen illegale online-inhoud', 1 maart 2018, online via: http://europa.eu/rapid/press-release_IP-18-1169_nl.htm (laatst geraad-pleegd op 3 maart 2018).

709 Balkin 2017, p. 1187.

gemakkelijk een vorm van indirecte overheidscensuur kan ontstaan, terwijl de Grondwet voorafgaande beperkingen van de uitingsvrijheid volledig verbiedt.[710] Ook leidt dit tot vragen voor wat betreft de rechtsbasis van dergelijke inperkingen van de vrijheid van meningsuiting en de voorzienbaarheid daarvan.[711]

III.3.2.4 Chilling effect

In paragraaf II.3.2.2 is al ingegaan op de voorwaarden voor beperking van de vrijheid van meningsuiting. Daarbij is aangegeven dat beperkingen, sancties en maatregelen volgens vaste rechtspraak van het EHRM niet zodanig van aard mogen zijn dat er een 'chilling effect' optreedt. Big Data-processen kunnen er echter wel degelijk toe leiden dat burgers hun gedrag aanpassen. Als een bericht mogelijk in strijd is met de interne richtlijnen van het platform, kunnen algoritmes het plaatsen van dat bericht verhinderen of ongedaan maken. De wetenschap dat content mogelijk wordt verwijderd kan ertoe leiden dat personen dergelijke content niet langer plaatsen, en ook dat ze in veel gevallen de 'veilige' kant kiezen. Dat betekent dat ze minder geneigd kunnen zijn om fel opiniërende, mogelijk grievende berichten te plaatsen of kunstzinnige, controversiële en maatschappijkritische uitingen als de foto van het Napalm-meisje. Doet dit zich voor, dan is dit precies het 'chilling effect' waar het EHRM voor waarschuwt.

Omvangrijke gegevensverzameling, dataopslag en -analyse leiden verder tot een verlies van anonimiteit op het Internet. Hierdoor kunnen mensen het gevoel hebben dat zij hun mening niet langer veilig online kunnen ventileren, en ook dat kan een 'chilling effect' hebben.[712]

Het Internet of Things kan ervoor zorgen dat dit effect ook wordt uitgebreid naar de offline wereld. Met het Internet verbonden apparaten verzamelen grote hoeveelheden informatie en zijn soms in staat om spraak te herkennen, op te slaan, te verwerken en te analyseren. De privacyvoorwaarden van Samsungs Smart-tv bevat onder meer de zin: 'Please be aware that if your spoken words include personal or other sensitive information, that information will be among the data captured and transmitted to a third party through your use of Voice Recognition.'[713] Ook dit kan leiden tot een zekere angst om zich vrijelijk te uiten, waardoor een mogelijk 'chilling effect' zich uitbreidt tot offline meningsuiting in de huiselijke sfeer.

---

710 De Staatscommissie Grondwet heeft in 2010 nog geadviseerd om het censuurverbod niet open te breken, bijvoorbeeld om extra bescherming van kinderen mogelijk te maken, vanwege de daarmee samenhangende risico's van beperking van de vrijheid van meningsuiting (Staatscommissie Grondwet 2010, p. 71 e.v.).

711 Wagner 2017, p. 13.

712 WRR 2016, p. 92 en 135.

713 Samsung Local Privacy Policy - SmartTV Supplement, via: http://www.samsung.com/hk_en/info/privacy/smarttv/ en daarover Internet Society 2015, p. 9 en 19.

III.3.3 Vrijheid van demonstratie

In paragraaf II.3.4 is al gebleken dat er een nauwe samenhang bestaat tussen de demonstratie- of betogingsvrijheid en het recht op vrijheid van meningsuiting. De demonstratievrijheid betreft vooral een collectief element: het gaat erom samen met anderen een mening naar voren te brengen. Veel van de hiervoor besproken effecten van nieuwe technologieën voor de vrijheid van meningsuiting gelden dan ook op dezelfde manier voor de demonstratievrijheid. Zo kunnen de snelle communicatiemogelijkheden van het Internet ervoor zorgen dat mensen elkaar gemakkelijk vinden en kunnen ze helpen bij het organiseren van protestacties, maar kan er ook sprake zijn van een 'chilling effect' of van private censuur die maakt dat mensen de noodzakelijke toegang tot informatie juist mislopen.

Meer specifiek relevant voor de demonstratievrijheid is wel dat Big Data-analyses een rol kunnen spelen bij de beslissingen die (lokale) overheden moeten nemen over het reguleren van een bepaalde, aangekondigde demonstratie. Er kan een algoritmisch risicoprofiel worden opgesteld van demonstraties, waarin de specifieke organisaties die melding maken van de organisatie en mogelijke deelnemers aan de organisatie worden opgenomen. De analyse van een grote hoeveelheid data over deze (rechs)personen kan ten grondslag worden gelegd aan een mogelijk verbod op de demonstratie of aan beperkende maatregelen. Dit kan ten gunste van de demonstratievrijheid uitpakken als daardoor een demonstratie met bepaalde, slimme veiligheidsmaatregelen toch doorgang kan vinden, terwijl die met beperktere informatie veiligheidshalve misschien zou zijn verboden. De problemen van bias en ondoorzichtigheid van informatie, die ook bij andere grondrechten een rol spelen, kunnen echter ook hier opspelen.

Van belang is verder dat het Internet of Things constante monitoring van demonstraties mogelijk maakt. In een slimme stad kunnen alarmsystemen, hekwerkdetectoren en camera's worden ingezet bij het reguleren van de demonstratie. Kunstmatige intelligentie, in de vorm van emotieherkenning, kan bovendien worden gebruikt om toekomstig gedrag van de (groep) demonstranten te voorspellen. Op basis van deze informatie en voorspellingen kan eventueel worden besloten tot het afgelasten van een demonstratie. Opnieuw geldt echter dat dit niet per definitie zal leiden tot grondrechtelijke knelpunten, of tot knelpunten die groter zijn dan wanneer een overheid op basis van 'analoge' gegevens beslissingen neemt over een demonstratie; ook hier kan een betere informatiebasis zelfs voordelig uitpakken. Nadelige effecten zijn in dit soort gevallen dan eerder gelegen in de bescherming van de privacy, in eventuele discriminerende effecten (bijvoorbeeld wanneer door een bias in algoritmes demonstraties van extreemlinkse groeperingen eerder worden verboden dan demonstraties van extreemrechtse groeperingen) en in ondoorzichtigheid van het besluitvormingsproces. Dit zijn grondrechtelijke knelpunten die niet zozeer in deze paragraaf, maar vooral hiervoor al aan bod zijn gekomen en hierna nog aan bod zullen komen.

III.3.4 Vrijheid van vereniging

De vrijheid van verenging beschermt onder meer de vrijheid van personen om lid te worden van een vereniging (positieve verenigingsvrijheid).[714] In dit verband is van belang dat door de proliferatie van Big Data-toepassingen niet alleen de overheid en grote commerciële bedrijven, maar ook particulieren en kleinere organisaties beschikken over de mogelijkheid om grootschalige data-analyses uit te voeren. Als verenigingen algoritmes inzetten om te bepalen wie er lid mag worden van vereniging rijzen er privacy-bezwaren, en tot op zekere hoogte ook bezwaren van ongelijke behandeling.[715] Als een algoritmisch besluit bepaalt dat een persoon niet wordt toegelaten tot een vereniging, is het bovendien lastig om het beslissingsproces te doorgronden en het besluit (in rechte) te bestrijden.[716] De bezwaren die vanuit andere grondrechten gelden voor dit soort handelen door de overheid, gelden dan in feite (op horizontaal niveau) ook voor handelen door verenigingen. De vrijheid van vereniging omvat onder meer het recht om zich te verenigen (de oprichtingsvrijheid). Tot op zekere hoogte kan de overheid echter eisen stellen aan de oprichting van nieuwe verenigingen.[717] Bij de beslissing van de overheid om een vereniging al dan niet te erkennen, of bijvoorbeeld aan te merken als politieke partij, kan gebruik worden gemaakt van Big Data-analyse en risicoprofielen van individuele leden van de vereniging. Hetzelfde geldt voor het eventueel verbieden of ontbinden van een bestaande vereniging. De overheid (in de hoedanigheid van het Openbaar Ministerie) is in staat om grote hoeveelheden data over de vereniging en haar leden te verzamelen en deze te analyseren. De uit analyse verkregen informatie kan worden ingezet ter ondersteuning van de stellingname dat de werkzaamheden van de vereniging in strijd zijn met de openbare orde. Dit geldt met name bij verenigingen waarbij veel (vermeende strafbare) activiteiten zich online afspelen.[718] Big Data kan zo een rol spelen bij inperking van de verenigingsvrijheid. Daarmee is overigens niet gezegd dat hier sprake is van een knelpunt; het is vooral zo dat door de werking van de nieuwe technologieën meer informatie kan worden verzameld en kan worden gebruikt. In dit soort gevallen is de zorg eerder gelegen in de toegankelijkheid van deze informatie en de gemaakte analyses voor de betrokken verenigingen, en in de daarmee samenhangende rechtsbescherming. De daarbij bestaande knelpunten komen nader aan de orde in paragraaf III.4.

714 Zie hoofdstuk II, par. 3.5.

715 Zie hoofdstuk II, par. 2; zie overigens ook wel Zoontjens 2006: de AWGB staat hieraan alleen in de weg voor zover het gaat om verenigingen die goederen en diensten aanbieden, maar niet voor zover het gaat om besloten verenigingen; op dit punt kan echter wel art. 1 Gw of art. 14 EVRM relevant zijn.

716 Zie hoofdstuk II, par. 4.

717 Zie hoofdstuk II, par. 3.5.2.

718 Zie de casus van Vereniging Martijn, verboden bij arrest van de Hoge Raad 18 april 2014, *NJ* 2014/507.

III.3.4 Kiesrecht

Toegang tot informatie tijdens de verkiezingscampagnes

Voor het goed kunnen uitoefenen van het actief en passief kiesrecht zijn het hebben van toegang tot diverse, onafhankelijke informatie en vrije meningsuiting essentieel. Enkele van de hiervoor in paragraaf III.3.2 aangeduide knelpunten kunnen daardoor ook de uitoefening van het actief en passief kiesrecht beïnvloeden. Het in paragraaf III.3.2.3 besproken 'chilling effect' en de mogelijkheden van indirecte censuur kunnen bijvoorbeeld raken aan de uitoefening van het actief kiesrecht. Als mensen weten dat hun online leesgedrag wordt gemonitord, dan kan dit ertoe leiden dat zij over bepaalde politieke onderwerpen geen nieuws of informatie meer durven te lezen.[719] Ook kan het zijn dat bepaalde informatie wordt weggefilterd als die maatschappelijk ongewenst wordt gevonden. Dit soort processen beïnvloedt de mate waarin burgers informatie tot zich kunnen nemen. Ook het gemakkelijke ontstaan van filterbubbels kan ertoe leiden dat kiezers eenzijdig worden geïnformeerd en dat zij de nodige onafhankelijkheid van informatie missen om een goede keuze te kunnen maken. Wereldwijd worden bovendien bots, algoritme-gedreven computerprogramma's, ingezet om het politieke discours op sociale media en andere online platforms te beïnvloeden. Zo bevat Twitter circa 30 miljoen accounts die 'bot-driven' zijn en menselijke gebruikers imiteren om (al dan niet *fake*-) informatie te verspreiden en het politieke debat te beïnvloeden. Zowel lobbyisten, activisten als politieke campagnestrategen gebruiken deze algoritme-gedreven opiniemakers die de politieke opvattingen van kiezers aanzienlijk kunnen beïnvloeden. Big Data stelt bots in staat om specifieke kiezersgroepen te adresseren.[720]

Belangrijk is verder dat Big Data-analyses politieke partijen in staat stelt om nauwkeurige kiezersprofielen op te stellen die gebruikt worden bij het bepalen van campagnestrategieën en het adresseren van kiezers.[721] Barack Obama deed dit tijdens de presidentiële verkiezingscampagnes in de VS,[722] de Brexiteers gebruikten Big Data in de aanloop naar het Brexit-referendum[723] en Donald Trump vertrouwde op de meest geavanceerde Big Data-technologie in zijn eigen campagne.[724] De eerder genoemde privacybezwaren van (met name) Big Data, doen hiermee hun intrede in het politieke domein. Bovendien kunnen de via Big Data gestuurde verkiezingscampagnes er in combinatie met de in paragraaf

719 Zuiderveen Borgesius e.a. 2016, p. 261.
720 Woolley & Howard 2016. Zie over de inzet van bots tijdens verkiezingsdebatten tussen Hillary Clinton en Donald Trump het artikel van Kollanyi, Howard & Woolley 2016.
721 Zie ook Staatscommissie Parlementair Stelsel 2017, p. 49.
722 Zie nader hoofdstuk I, par. 2.2.1 en 2.3.1.
723 Origineel vindbaar via: http://leave.eu/en/news/2015-11-20/the-science-behind-our-strategy, nu gearchiveerd op: https://archive.li/rN22u.
724 Grasseger & Krogerus 2017.

III.3.2 besproken processen toe leiden dat burgers onvoldoende diverse en pluriforme informatie over hun keuzes ontvangen van de politici die aan de verkiezingen deelnemen en die deze burgers zullen gaan representeren.

De algoritmes van grote bedrijven als Google kunnen eveneens grote invloed hebben op de uitoefening van het actief kiesrecht.[725] De algoritmes van Facebook, Twitter of Google bepalen immers wat gebruikers lezen en welke informatie tot hen komt. Daardoor zijn het niet alleen campagnemakers, maar vooral ook deze bedrijven die de kiezer kunnen beïnvloeden. Iedere verandering in de algoritmes die deze bedrijven gebruiken raakt immers het denken van kiezers, waaronder hun bereidheid om te gaan stemmen en politieke keuzes in het stemhokje. In een reactie liet Google weten dat van een dergelijke politieke invloed geen enkele sprake was: 'Google has never ever re-ranked search results on any topic (including elections) to manipulate user sentiment. Moreover, we do not make any ranking tweaks that are specific to elections or political candidates.'[726] Het onderzoek toont echter wel het *potentiële* effect van manipulatie van algoritmes gebruikt door zoekmachines aan.

In een vergaand scenario is het niet menselijke beïnvloeding van algoritmes, maar het zelflerende karakter van het algoritme dat de manipulatie bewerkstelligt en dat bepaalde partijen of kandidaten naar de top van zoekresultaten stuwt. De zelfstandige keuzevrijheid van het individu, die hij op basis van goede informatie kan uitoefenen, is dan sterk gereduceerd en de onderliggende rationale van het kiesrecht wordt vergaand aangetast. In de woorden van Epstein: 'Under this scenario, a *computer program* is picking our elected officials.'[727]

Passief kiesrecht

Tot op zekere hoogte kan ook het passief kiesrecht worden beïnvloed door nieuwe technologieën. Dit kan vooral gebeuren als politieke partijen de geschiktheid van potentiële kandidaten gaan bepalen aan de hand van Big Data-analyse. De mechanismen die zijn besproken in paragraaf III.2 kunnen dan immers leiden tot ongerechtvaardigde uitsluiting en indirecte discriminatie.

Beïnvloeding van de opkomst

Algoritmische aanmoedigingen om te gaan stemmen hebben daadwerkelijk invloed op de opkomst bij verkiezingen. Een experiment met stemherinneringen tijdens de verkiezingen voor het Amerikaanse Congres in 2010 liet zien dat circa 340.000 extra personen naar de stembus gingen als gevolg van de stemoproep van Facebook.[728] In landen of gebieden waar

725 Epstein 2015.
726 Singhal 2015.
727 Epstein 2015.
728 Bond e.a. 2012.

kiezersregistratie verplicht was, kregen gebruikers waarvan Facebook dacht dat zij kiesgerechtigd waren, herinneringen om zich te registreren.[729] Op verkiezingsdagen kregen gebruikers herinneringen om te gaan stemmen en zagen zij berichten over de ervaringen van vrienden tijdens de verkiezingen. Gebruikers konden deze berichten handmatig uitzetten, maar veel mensen zullen deze berichten toch hebben lezen.[730] Op zichzelf kan het als positief worden beoordeeld als mensen door deze aanmoedigingen gestimuleerd worden hun kiesrecht actief te gebruiken. Bij referenda is het al dan niet halen van de opkomstdrempel echter een belangrijk politiek strijdpunt. Stemoproepen met behulp van Big Data en algoritmes zijn in een dergelijke referendumssituatie niet neutraal, maar per definitie politiek gekleurd.

Daarnaast kunnen de door Big Data en algoritmes mogelijk gemaakte aanmoedigingen gekleurde effecten hebben als politieke actoren groots inzetten op beïnvloeding van zoekmachines en sociale media. Zo probeerde Donald Trump de stembusgang van Afro-Amerikanen te ontmoedigen tijdens de presidentsverkiezingen in 2016. Hiertoe gebruikte hij de resultaten van grootschalige data-analyse om zogeheten 'dark posts' (niet-publieke, op een specifieke groep gerichte berichten) naar deze groep kiezers te versturen.[731] Dergelijke op specifieke kiezersgroepen gerichte pogingen om stemmen te ontmoedigen, zijn laakbaar vanuit het gezichtspunt van vrije en geheime verkiezingen. Bovendien kan het met behulp van algoritmes bewerkstelligen van een bepaalde verkiezingsopkomst politieke gevolgen hebben die eveneens leiden tot een minder betrouwbare uitkomst. Zo leidt een hoge opkomst ertoe dat politieke partijen met een trouwe, oudere achterban, een relatief lager aantal stemmen krijgt. Bij verkiezingen binnen een vertegenwoordigend systeem kan dit al een vertekend beeld geven, maar mogelijk nog problematischer is een dergelijke oneevenwichtigheid bij referenda.

Gedrag in het stemhokje

Zoekmachines en sociale media kunnen aanzienlijke invloed hebben op de politieke keuzes die kiezers maken in het stemhokje. In een experiment toonde Facebook aan het emoties van gebruikers kon beïnvloeden door de weergave van informatie in de Newsfeed te manipuleren.[732] Dergelijke manipulatie op een verkiezingsdag kan de politieke voorkeuren van kiezers bepalen en daarmee raken aan de uitoefening van het actief kiesrecht. Een onderzoek van Epstein en Robertson richtte zich specifiek op de politieke impact die

729 Griffin 2016.

730 Facebook Helpcentrum, 'Waar kan ik informatie over verkiezingen en stemmen vinden op Facebook?' via: https://nl-nl.facebook.com/help/1519550028302405.

731 Tufekci 2018. Zie ook 'Silicon Valley creëerde de eerste Twitter-president. Nu kijkt het de andere kant op', *De Volkskrant* 21 januari 2018, via https://www.volkskrant.nl/buitenland/silicon-valley-creeerde-de-eerste-twitter-president-nu-kijkt-het-de-andere-kant-op~a4560688/. Zie nader over dergelijke vormen van online political microtargeting: Zuiderveen Borgesius e.a. 2018.

732 Kramer, Guillory & Hancock 2014, p. 8788-8790.

manipulatie van zoekmachines kan hebben.[733] Het blijkt dat zoekmachines door het aanpassen van zoekresultaten het stemgedrag van 20% van de zwevende kiezers kunnen wijzigen. Dit percentage kan bovendien hoger zijn onder specifieke groepen kiezers, zoals mensen met een gebrekkige politieke kennis. Op basis van grote hoeveelheden data is het mogelijk dergelijke groepen specifiek te identificeren en te adresseren. Dergelijke aanpassingen van zoekresultaten zijn niet zichtbaar voor kiezers, waardoor zij zich niet bewust zijn van manipulatie. Ook hierdoor wordt het kiesrecht evident geraakt en is het nog maar de vraag of sprake is van de gewenste 'vrije en geheime verkiezingen'.

III.4 Procedurele rechten

III.4.1 Inleiding

Nieuwe technologieën zijn binnen de rechtspleging op vele manieren steeds belangrijker. Big Data-analyses kunnen behulpzaam zijn bij politieonderzoek en opsporing. Bewijsmateriaal dat door middel van dit soort analyses is verkregen, kan vervolgens een rol spelen in het strafproces. Big Data- en KI-technologieën kunnen de rechter ook helpen bij zijn besluitvorming en ze kunnen een deel van zijn taken zelfs overnemen. Ook in bestuursrechtelijke en civielrechtelijke procedures komt steeds meer betekenis toe aan informatie die is verkregen door Big Data-analyses, of kan een burger besluiten proberen aan te vechten die op basis van algoritmes zijn genomen.

Deze ontwikkelingen leveren tal van vragen op vanuit het perspectief van het recht op een effectief rechtsmiddel en toegang tot de rechter, en vanuit het perspectief van het recht op een eerlijk proces. Sommige ontwikkelingen zijn daarbij overwegend positief. Zo kan het zijn dat de inzet van nieuwe technologieën ervoor zorgt dat procedures efficiënter verlopen en ze daardoor binnen redelijke termijn kunnen worden afgerond. Andere ontwikkelingen zetten de procedurele rechten echter onder druk.

In deze paragraaf worden de verschillende in hoofdstuk I besproken technologische ontwikkelingen bezien vanuit het perspectief van de procedurele grondrechten. De inhoud van deze rechten is in hoofdstuk II kort uiteengezet, waarbij een onderscheid is gemaakt tussen het recht op een effectief rechtsmiddel en op toegang tot de rechter enerzijds, en anderzijds het recht op een eerlijk proces. Deze indeling zal ook in deze paragraaf worden aangehouden. Lang niet alle aspecten van de onderscheiden rechten komen daarbij aan bod; de focus ligt op die rechten waarop nieuwe technologieën daadwerkelijk impact (kunnen) hebben.

733 Epstein e.a. 2017; Epstein & Robertson 2015.

III.4.2 Recht op een effectief rechtsmiddel en op toegang tot de rechter

III.4.2.1 Transparantie van besluiten en effectieve toegang

Zoals in hoofdstuk II is omschreven, is het recht op een effectief rechtsmiddel en op toegang tot de rechter wezenlijk in een democratische rechtsstaat. Niet in het minst is dat het geval omdat een rechterlijke voorziening individuen de mogelijkheid biedt om de andere, in eerdere paragrafen besproken grondrechten te laten beschermen tegen handelen van de overheid of van derden. In hoofdstuk II is duidelijk geworden dat het recht op een effectief rechtsmiddel en toegang tot de rechter een groot aantal facetten kent. Duidelijk is daarbij dat procedurele zorgvuldigheidseisen niet alleen worden gesteld aan een procedure bij de rechter. Bestuurlijke en regelgevende processen die leiden tot ingrijpende beslissingen moeten eveneens aan bepaalde zorgvuldigheidsstandaarden voldoen, net als bestuurlijke voorprocedures. Eisen van transparantie, participatie en zorgvuldigheid zijn daarbij in het bijzonder van belang. Precies op deze punten kunnen algoritme-gedreven beslissingen problematisch zijn. Dat geldt vooral waar het voor rechtszoekenden niet duidelijk is hoe de algoritmes precies hun werk doen of waar een Big Data-analyse automatisch leidt tot een ingrijpende beslissing, zonder dat mensen hierover tijdig worden gehoord. Enkele van deze 'black box'-problemen is al besproken in paragraaf III.1 over privacy en in paragraaf III.3 over het recht op toegang tot informatie.

In verband met het recht op een effectief rechtsmiddel en de toegang tot de rechter, is een specifiek onderwerp het bespreken waard, omdat dit nauw verband houdt met het recht op toegang tot informatie over ingrijpende beslissingen. Hildebrandt heeft beredeneerd dat het recht op toegang tot een effectief rechtsmiddel impliceert dat wanneer algoritmische beslissingen worden genomen, het subject van deze beslissingen 'know[s] about the existence of such decisions', omdat 'a person cannot contest incorrect or unfair decisions that impact her life if she has no clue that (…) decisions have been reached.'[734] Daarnaast heeft het EHRM aangenomen, zoals in hoofdstuk II verder uiteengezet, dat wanneer een bestuursbesluit onvoldoende draagkrachtig of transparant is onderbouwd, het voor de rechtszoekende onmogelijk is om dit besluit effectief aan te vechten bij de rechter. Goede, transparante en kenbare motivering van beslissingen die inbreuk maken op grondrechten, is daarmee altijd nodig.

In verband met algoritme-gedreven beslissingen kan vooral een probleem ontstaan als een bedrijf of een bestuursorgaan weigert inzicht te geven in het algoritme, bijvoorbeeld omdat dit concurrerende ondernemingen in de kaart speelt of omdat openbaarmaking van de werking van het algoritme veiligheidsrisico's met zich meebrengt. Zo heeft Meuwese gewezen op een voorbeeld waarbij scholen gebruik konden maken van een Big Data-toe-

734 Hildebrandt 2015, p. 101.

passing die bepaalde of leerkrachten goed genoeg waren om hun baan te houden. Hierbij werd gemeten wat het aandeel van een leerkracht was in de testresultaten van kinderen.[735] Dit systeem leidde tot het ontslag van een populaire leerkracht, wiens score volgens het model te laag was. Het algoritme dat verantwoordelijk was voor de Big Data-analyse kon niet inzichtelijk worden gemaakt, omdat er een licentieovereenkomst was gesloten met de programmeur van het algoritme. Voor de ontslagen leerkracht maakte dit het onmogelijk om het genomen besluit beargumenteerd aan te vallen. In het licht van de rechtspraak van het EHRM is duidelijk dat de effectieve toegang tot de rechter hierdoor wordt geraakt.

Het risico dat beslissingen worden genomen zonder medeweten van het object doet zich verder voor bij algoritmische profilering en datamining. Zo kan algoritmische profilering leiden tot het opstellen van profielen die (al dan niet indirect) verbonden zijn met verdachte gronden als ras of seksuele gerichtheid. Aan de hand van dergelijke profielen kan online-prijsdifferentiatie plaatsvinden of kan besloten worden om personen die voldoen aan het profiel bepaalde aanbiedingen of vacatures niet toe te sturen. Voor de toegang tot de bestuursrechter is bovendien belangrijk dat in de bestuursrechtelijke sfeer kan worden besloten dat iemand niet in aanmerking komt voor een socialezekerheidsuitkering of een sociale voorziening. In dergelijke gevallen worden iemands toekomstige handelingsopties beïnvloed door discriminatoire profielen of worden zelfs bepaalde grondrechten aangetast, zoals het recht op respect voor de persoonlijke autonomie of het recht op non-discriminatie.[736] Als mensen echter niet op de hoogte zijn van dit soort vormen van besluitvorming, of wanneer zij geen inzicht hebben in het soort processen dat leidt tot een voor hen benadelend effect, zal het voor de betrokkenen erg moeilijk zijn om hun recht te halen.[737] In het geval van dergelijke 'ongemerkte' of in ieder geval niet transparant onderbouwde grondrechtenschendingen, kan het recht op een effectief rechtsmiddel in het geding zijn.

III.4.2.2 Een onafhankelijke en onpartijdige rechter

Het recht op toegang tot de rechter impliceert dat de rechter onafhankelijk en onpartijdig kan oordelen.[738] In dit verband is van belang dat de inzet van KI en Big Data een aanzienlijke invloed kan hebben op de beoordeling van rechtszaken, zoals in hoofdstuk I ook al is geïllustreerd.[739] Daarbij geldt dat deze invloed in een aantal gevallen heel positief is. KI kan bijvoorbeeld fungeren als een waardevolle 'sparring partner' voor rechters. Computers kunnen helpen om argumenten te wegen of zwakke plekken in juridische argumentatie

735 Meuwese 2017, p. 161.
736 Moerel & Van der Wolk 2017, p. 41-46.
737 Ook het recht op persoonlijke autonomie kan in dergelijke gevallen in van *behavioural targeting* in het geding zijn, zonder dat slachtoffers hiervan op de hoogte zijn.
738 Zie hoofdstuk II, par. 4.2.
739 Zie meer algemeen over de eisen van een onafhankelijke en onpartijdige rechter hoofdstuk II, par. 4.2.

aan te geven, waardoor een rechter tot meer objectieve en beter onderbouwde oordelen kan komen.[740] Rechterlijke oordeelsvorming kan ook ondersteund worden door algoritmes die vonnissen en arresten met elkaar vergelijken en afzetten tegen informatie over een voorliggende zaak. Rechters krijgen zo inzicht in overeenkomsten en verschillen tussen zaken, waardoor gelijke gevallen gelijk(er) beoordeeld kunnen worden en de consistentie van rechtspraak wordt vergroot. Op die manier kan KI ook bijdragen aan de consistentie van de rechterlijke oordeelsvorming in strafzaken. Het is bijvoorbeeld mogelijk om de strafmaat in strafzaken te vergelijken, inzicht te krijgen in de factoren die in straftoemeting een rol spelen of te achterhalen in welk type zaken ruimte is voor standaardvonnissen. Dergelijke algemene inzichten kunnen vervolgens worden meegenomen in voorliggende zaken. In dergelijke gevallen helpt KI bij het nemen van een beslissing in concrete zaken.[741]

Naarmate de invloed van KI bij het bepalen van de uitkomst in concrete zaken groter wordt, komt echter ook een aantal knelpunten in beeld. Twee voorbeelden kunnen dit inzichtelijk maken:

- Een treffende illustratie biedt allereerst een kwestie die zich voordeed in de Amerikaanse staat Wisconsin.[742,743] Bij het beoordelen van de strafmaat in de strafzaak tegen Eric Loomis maakte de rechter gebruik van het COMPAS-systeem. Dit data-gedreven systeem laat algoritmes bepalen hoe hoog het risico op recidive van een verdachte is. De uitkomst van Big Data-analyse liet in het geval van Loomis zien dat de kans op recidive hoog was. Dit beïnvloedde de straftoemeting, waardoor Loomis werd veroordeeld tot zes jaar cel. Een privaat bedrijf was eigenaar van het systeem, waardoor het noch voor de rechter noch voor Loomis mogelijk was om inzicht te krijgen in de werking van het algoritme.
- Dichter bij huis – en buiten de context van het strafrecht – heeft robotrechter *e-court*, een digitaal, privaat scheidsgerecht, recentelijk stof doen opwaaien.[744] De term 'robotrechter' wordt in dit verband gebruikt om algoritmes aan te duiden die geautomatiseerde

740 Prakken 2018, p. 274.

741 Prins & Van der Roest 2018, p. 263-264.

742 Zie *State v. Loomis*, 881 N.W.2d 749 (Wis. 2016); Loomis diende een *petition for certiorari* in bij het federale Hooggerechtshof, maar deze werd afgewezen (zie http://www.scotusblog.com/case-files/cases/loomis-v-wisconsin/0; laatst geraadpleegd 2 februari 2018). Dit betekent dat het Hooggerechtshof geen oordeel over de zaak zal vellen.

743 Een soortgelijk voorbeeld zou zich voor kunnen doen in de staat New Jersey, waar sinds 2017 gebruik gemaakt van een algoritmische risicobeoordeling om te bepalen of een verdachte op borgtocht vrij mag komen; zie New York Times 2017.

744 'Vonnis te koop. Private rechtspraak in de incasso-industrie', *De Groene Amsterdammer* 17 januari 2018, online via: https://www.groene.nl/artikel/vonnis-te-koop (laatst geraadpleegd 2 februari 2018) en 'Rechters bezorgd over spotgoedkope, private rechtspraak', *Trouw* 18 januari 2018, online via: https://www.trouw.nl/home/rechters-bezorgd-over-spotgoedkope-private-rechtspraak-~aec4584f/ (laatst geraadpleegd 2 februari 2018). Al eerder werd in juridische literatuur aandacht besteed aan e-court. Zie onder meer Jongbloed 2014 en Hartendorp 2014.

oordeelsvorming en motivering mogelijk maken. Een groot aantal verzekeraars en andere bedrijven (als Bol.com) heeft in de algemene voorwaarden opgenomen dat geschilbeslechting plaatsvindt door middel van arbitrage (art. 1020 e.v. Rv) of bindend advies (art. 7:900 BW) door *e-court*.Reeds sinds 2011 is bij *e-court* sprake van automatische afdoening van geschillen in zaken die zien op schuldinning waarin de schuldenaar geen verweer voert.[745] Ook hier is het voor partijen moeilijk om inzicht te krijgen in de werking van het algoritme waardoor de robotrechter wordt gedreven.

In beide voorbeelden komen grondrechtelijke knelpunten voort uit het 'black box'-karakter van (zelflerende) algoritmes. Hierna wordt nog afzonderlijk ingegaan op de gevolgen hiervan op het recht op een eerlijk, open en evenwichtig proces en het recht op een kenbare en draagkrachtige motivering van het rechterlijk oordeel. Voor nu is van belang dat rechterlijke oordeelsvorming op basis van ondoorzichtige KI-toepassingen een negatieve impact kan hebben op de onafhankelijkheid en onpartijdigheid van de rechter.[746] De rechterlijke onafhankelijkheid omvat mede beslissingsvrijheid in concrete zaken (functionele onafhankelijkheid), terwijl onpartijdigheid vergt dat een rechter onbevooroordeeld tegenover een zaak staat.[747] Deze onafhankelijkheid en onpartijdigheid kunnen in het gedrang komen wanneer rechters te veel vertrouwen op de KI en de algoritmes die hen ondersteunen in oordeelsvorming. Als een algoritme door of onder verantwoordelijkheid van een ander overheidsorgaan is geprogrammeerd en de rechter dit klakkeloos volgt, staat hij allicht niet meer volledig onafhankelijk tegenover de zaak. Bovendien is in hoofdstuk I uiteengezet dat ongemerkt *biases* in een algoritme kunnen sluipen die in het nadeel kunnen zijn van een van de procespartijen. Daarop is uitgebreid ingegaan in paragraaf III.2 over het gelijkheidsbeginsel en het verbod van discriminatie. De ondoorzichtigheid van algoritmes kan betekenen dat deze *biases* terechtkomen in de rechterlijk oordeelsvorming en dat ze de blik van de rechter onterecht kleuren.

III.4.3 Recht op een eerlijk proces

Is eenmaal toegang verkregen tot een proces voor de rechter, dan moet dit proces eerlijk verlopen. In hoofdstuk II is uiteengezet wat de belangrijkste procedurele waarborgen zijn die samenhangen met dit recht op een eerlijk proces: (1) het recht op afronding van de procedure binnen redelijke termijn, (2) de eerlijkheid, openheid en evenwichtigheid van de procedure, (3) de beschikbaarheid van een voldoende kenbare en draagkrachtige

745 Zie Nakad-Weststrate e.a. 2015, p. 1102-1112: 'the e-Court judgments by default in debt collection proceedings – are no longer the product of any human reasoning; the verdicts are rendered as the sole result of AI.'

746 Zie in deze trant Prins & Van der Roest 2018, p. 265.

747 Zie hoofdstuk II, par. 4.2.

motivering voor de rechterlijke beslissing, en (4) een aantal specifieke waarborgen die gelden in strafrechtelijke procedures. De invloed van nieuwe technologieën op deze procedurele waarborgen en rechten komen hierna achtereenvolgens aan bod.

III.4.3.1 Afronding van een procedure binnen redelijke termijn

Een positief effect kan worden bewerkstelligd als Big Data wordt ingezet ter verbetering van de rechtspleging of bedrijfsvoering bij gerechten. Van Ettekoven en Marseille hebben er bijvoorbeeld op gewezen dat de analyse van Big Data over aantallen zaken, aantal en soort beroepsgronden per zaak, doorlooptijden, het aantal ingeschakelde deskundigen, proceskosten en cassatieberoepen weinig problematisch is.[748] Deze gegevens worden immers ook zonder Big Data-analyse verzameld en geanalyseerd, zij het met enige moeite. Wordt op dit punt Big Data ingezet, dan kan dit leiden tot een verhoging van de efficiëntie van de rechtspraak en daarmee tot verhoging van het aantal zaken dat binnen redelijke termijn wordt afgedaan.

III.4.3.2 Open, eerlijk en evenwichtig proces

In hoofdstuk II is een set van procedurele rechten uiteengezet die kunnen worden samengenomen onder de noemer van het recht op een open, eerlijke en evenwichtige procedure. Dit betekent onder meer dat moet worden voorzien in *equality of arms*: geen van de bij een rechtsgeding betrokken partijen mag de overhand krijgen, bijvoorbeeld door een informatievoordeel, of mag juist in een nadelige positie terecht komen, bijvoorbeeld omdat hij bepaalde informatie of voorzieningen niet krijgt die de andere partij wel heeft. Algoritme-gedreven besluitvorming draagt duidelijke risico's in zich voor de evenwichtigheid van de procedure. Dit houdt verband met het hiervoor al genoemde en in hoofdstuk I meer uitgebreid besproken 'black box-karakter' van algoritmes. Algoritmes en algoritme-gedreven besluitvorming zijn vaak ondoorzichtig door hun technologische en contextuele complexiteit, met name in een Big Data-context. Hierdoor zijn de uitkomsten van algoritmes *ex post* lastig uit te leggen. Dit wordt versterkt doordat de exacte instructies van het algoritme om commerciële of veiligheidsredenen veelal geheim worden gehouden. In paragraaf III.4.3 is al aangegeven dat deze ondoorzichtigheid een belemmering kan vormen voor het recht op een effectief rechtsmiddel of op toegang tot de rechter, omdat mensen hierdoor niet altijd op de hoogte zijn van algoritmisch voorbereide publieke of private beslissingen. Waar dat wel het geval is, is het voor hen niet altijd gemakkelijk om te achterhalen op welke gronden zo'n beslissing is gebaseerd en hoe een eis of klacht dan vorm moet krijgen. Ook als wel toegang tot de rechter is verkregen, kan zich bovendien een aantal situaties voordoen waar het recht op een open, eerlijk en evenwichtig proces onder druk komt te staan.

748 Van Ettekoven & Marseille 2017, p. 261-262.

- Een eerste probleem is dat in een rechterlijke procedure sprake kan zijn van een ongelijke informatiepositie van procespartijen. De WRR wees er al op dat de burger vaak niet voldoende technologische kennis en inzicht heeft om te weten hoe hij zich moet verdedigen in een zaak waarin algoritmes, computersystemen en profielen een hoofdrol spelen.[749] Dit geldt onder meer voor de verdediging in strafzaken, wanneer het bewijs tegen een verdachte gebaseerd is op een Big Data-analyse. Het zal voor de verdediging, zeker als sprake is van gefinancierde rechtsbijstand, veelal ondoenlijk zijn de complexe, technologische Big Data-analyses te doorgronden die ten grondslag liggen aan het bewijs.[750] De overheid heeft in dergelijke zaken een dusdanige technologische voorsprong op de verdediging, dat vrijwel zeker sprake zal zijn van *inequality of arms*. Dit geldt ook bij bewijs dat verzameld is met behulp van apparaten die onderdeel uitmaken van het Internet of Things. In een artikel met de titel 'Een koelkast als getuige' wijst Prins op de belangrijke rol die het IoT kan (gaan) spelen bij de opsporing van strafbare feiten, bijvoorbeeld doordat via de dataverzameling door apparaten in de buurt van een verdachte informatie wordt verkregen die relevant is voor het strafrechtelijk onderzoek. Het is voor de verdediging in strafzaken van groot belang de betrouwbaarheid en rechtmatigheid van bewijs verzameld door middel van IoT-objecten te kunnen toetsen. Hiervoor is inzicht in de technologische werking van deze objecten noodzakelijk, en er zijn bijna onvermijdelijk technologische vragen die de verdediging niet zelfstandig zal kunnen beantwoorden.[751] Dergelijke kwesties beperken zich niet tot het strafrecht. Voor het bestuursrecht en het civiele recht zijn ze evenzeer relevant. Ook algoritmes gebruikt door bestuursorganen of werkgevers zullen immers tot op een zekere hoogte oncontroleerbaar zijn voor de gewone rechtzoekende en hun advocaten, waardoor zij een onvermijdelijk 'black box'-gehalte hebben en er een ongelijke informatiepositie ontstaat.[752]
- Een tweede probleem is dat algoritmische besluitvorming dusdanig complex kan zijn dat deze noch voor de procespartijen, noch voor de rechter te begrijpen is. Dit kan ertoe leiden dat de rol van deskundige computerexperts een prominente(re) rol gaat spelen in rechtszaken. Er bestaat dan een risico dat de financiële positie van procespartijen of het overwicht van een sterke procespartij als de staat een belangrijke rol gaat spelen bij de mogelijkheden om dergelijke deskundigen op te roepen. Als dit niet voldoende wordt gecontroleerd en gecompenseerd, kan dit opnieuw leiden tot *inequality of arms*.
- Als zelfs computerexperts de algoritmische besluitvorming niet meer kunnen doorgronden, ontstaat een derde probleem. De procespartij die de bewijslast ten aanzien van

749 WRR 2016, p. 22. Zie ook Steenbruggen & Zwenne 2017, p. 89-90.
750 Dijkstra e.a. 2016, p. 70.
751 Prins 2017.
752 Meuwese 2017, p. 165.

een specifiek punt draagt, draagt namelijk ook het bewijsrisico. Als deze procespartij er niet in slaagt aan de bewijslast te voldoen, bijvoorbeeld doordat het simpelweg onmogelijk is om het algoritmische besluitvormingsproces te doorgronden, zal de rechter geen rechtsgevolgen kunnen verbinden aan de stellingname van deze procespartij. In het strafrecht kan het dan voorkomen dat de verdediging er niet in slaagt aan te tonen dat bewijs dat is gegrond op Big Data-analyse, onrechtmatig is verkregen. Nu het op grond van artikel 359a Sv aan de verdediging is om te stellen en te onderbouwen dat sprake is van een vormverzuim, zal de rechter niet over kunnen gaan tot, bijvoorbeeld, bewijsuitsluiting.[753] Dit probleem beperkt zich bovendien niet tot het strafrecht.[754] Vooral in het bestuursrecht kunnen zelflerende Big Data-algoritmes een bron van zorg worden. Als sprake is van de verzameling van *real-time* data, verandert de dataset immers constant. Het uitvoeren van een *ex-tunc*-rechtmatigheidstoets kan daardoor voor de bestuursrechter lastig worden, omdat hij zal moeten beschikken over de gegevens zoals die zijn gebruikt ten tijde van het aangevochten besluit.[755] Als het algoritme zichzelf door *Machine Learning* aan kan passen op basis van eerder behaalde resultaten, is een dergelijke toets vrijwel onmogelijk.

– Ten slotte kan worden vastgesteld dat rechtspraak op basis van algoritmes afbreuk kan doen aan de openheid van het proces. Processen die oorspronkelijk in alle openbaarheid plaatsvonden en waarbij voor iedereen kenbaar was welke informatie en argumenten de rechter zou meenemen in zijn besluitvorming, kunnen in theorie immers door ondoorzichtige algoritmes worden overgenomen.[756] Dergelijke kritiek is onder meer ten aanzien van het hiervoor al genoemde *e-court* geuit.[757]

De hierboven geschetste problemen hebben zich reeds gemanifesteerd in de rechtspraak, zij het in beperkte mate. In een uitspraak van mei 2017 oordeelde de Raad van State bijvoorbeeld over besluiten over de zogenaamde Programmatische Aanpak Stikstof die gebaseerd zijn op Big Data.[758] Het computerprogramma PAS AERIUS ondersteunt de Programmatische Aanpak Stikstof. Dit computerprogramma bepaalt mede of iemand een vergunning krijgt voor een stikstofverhogende activiteit, zoals het uitbreiden van een veehouderij. AERIUS is een Big Data-toepassing.[759] De algoritmes van AERIUS maken

753 Zie over de strenge lijn die de Hoge Raad aanhoudt onder meer Brinkhoff 2016.

754 Over bewijslastverdeling in het bestuursrecht zie Schuurmans 2005. In civiele zaken is de hoofdregel neergelegd in artikel 150 Rv: 'De partij die zich beroept op rechtsgevolgen van door haar gestelde feiten of rechten, draagt de bewijslast van die feiten of rechten, tenzij uit enige bijzondere regel of uit de eisen van redelijkheid en billijkheid een andere verdeling van de bewijslast voortvloeit.'

755 Van Ettekoven & Marseille 2017, p. 260.

756 Hierover Markou 2017.

757 Landelijke Organisatie Sociaal Raadslieden 2018, p. 14.

758 ABRvS 17 mei 2017, *Computerrecht* 2017/256 m.nt. B.M.A. van Eck.

759 Zie in dit kader Van Ettekoven & Marseille 2017, p. 260.

berekeningen van stikstofdepositie op basis van een groot aantal gegevens, zoals geografische data, data over Natura 2000-gebieden en emissiedata van de sectorenindustrie, landbouw en wegverkeer. Daarbij wordt zoveel mogelijk gebruik gemaakt van actuele gegevens.[760] In zijn uitspraak overwoog de Raad van State het volgende:

> 14.3. Indien belanghebbenden rechtsmiddelen willen aanwenden tegen op het PAS gebaseerde besluiten kan daardoor een ongelijkwaardige procespositie van partijen ontstaan. Zij kunnen in geval van besluitvorming op basis van een programma dat vanuit hun perspectief is te beschouwen als een zogenoemde "black box" immers niet controleren op basis waarvan tot een bepaald besluit wordt gekomen en of de zekerheid bestaat dat het project of andere handeling de natuurlijke kenmerken van Natura 2000-gebieden niet zal aantasten.
> 14.4. Ter voorkoming van deze ongelijkwaardige procespositie rust in dit geval op genoemde ministers en de staatssecretaris de verplichting om de gemaakte keuzes en de gebruikte gegevens en aannames volledig, tijdig en uit eigen beweging openbaar te maken op een passende wijze zodat deze keuzes, gegevens en aannames voor derden toegankelijk zijn. Deze volledige, tijdige en adequate beschikbaarstelling moet het mogelijk maken de gemaakte keuzes en de gebruikte gegevens en aannames te beoordelen of te laten beoordelen en zo nodig gemotiveerd te betwisten, zodat reële rechtsbescherming tegen besluiten die op deze keuzes, gegevens en aannames zijn gebaseerd mogelijk is, waarbij de rechter aan de hand hiervan in staat is de rechtmatigheid van deze besluiten te toetsen.

De overwegingen van de Raad van State zijn geënt op het recht op *equality of arms* en het daaruit voortvloeiende gegeven dat besluitvorming door bestuursorganen geen *black box* mag zijn voor burgers. De uitspraak toont aan dat de Afdeling algoritme-gedreven besluitvorming beschouwt als een reëel gevaar voor de verwezenlijking van het recht op *equality of arms* en daarmee voor het recht op een eerlijk proces. De Afdeling verbindt hieraan de conclusie dat bestuursorganen inzicht moet bieden in de werking van het onderliggende algoritme om effectieve rechtsbescherming mogelijk te maken.

De civiele rechter lijkt (nog) niet zo ver te willen gaan. In een recente uitspraak oordeelde de Rechtbank Amsterdam over een lotingsalgoritme dat bepaalt welk kind op welke middelbare school wordt geplaatst.[761] In de procedure vorderden enkele ouders van uitgelote leerlingen om 'een analyse over de match die op basis van beschikbaar en gewenst aanbod

760 Zie hierover nader de webpagina van het Ministerie van Landbouw, Natuur en Voedselkwaliteit over PAS: https://www.synbiosys.alterra.nl/natura2000/gebiedendatabase.aspx?subj=pas&deel=1 (laatst geraadpleegd 3 januari 2018).

761 Rb Amsterdam 31 mei 2017, ECLI:NL:RBAMS:2017:3772.

is gemaakt.' Daarmee eisten zij inzicht in de werking van het matchingsalgoritme. De Rechtbank besliste negatief op de vordering op de (formalistische) grond dat artikel 843 Rv hier geen aanspraak op geeft, omdat 'eisers geen afgifte van bepaalde bescheiden' vorderden, 'maar beantwoording van een reeks vragen.' Los van de vraag of hier sprake is van Big Data, is de uitspraak interessant, omdat de uitspraak van de Rechtbank in zekere zin 'tegengesteld' is aan het oordeel van de Afdeling Bestuursrechtspraak.[762] De impact die algoritmische besluitvorming kan hebben op het recht op *equality of arms* wordt door de Rechtbank Amsterdam in mindere mate erkend dan door de Afdeling Bestuursrechtspraak.

III.4.2.4 Transparante en draagkrachtige motivering

Onderdeel van het recht op een eerlijk proces is dat rechterlijke uitspraken voldoende draagkrachtig en kenbaar worden gemotiveerd.[763] Dit houdt onder meer in dat de gronden waarop een beslissing berust in voldoende mate duidelijk moeten zijn voor de partijen en voor een hogere rechter. KI is in juridische kwesties tot op heden waarschijnlijk onvoldoende in staat om het eigen beslissingsproces adequaat te motiveren.[764] De enkele verwijzing naar de uitkomst van een algoritme, bijvoorbeeld ten aanzien van de strafmaat, zou daarmee op gespannen voet komen te staan met het recht op een voldoende gemotiveerd vonnis. Gezien het 'black box'-karakter van algoritmes is het bovendien de vraag of rechters een algoritmische beslissing die ten grondslag ligt aan een uitspraak in voldoende mate kunnen uitleggen.[765]

III.4.2.5 De onschuldpresumptie

Artikel 6 lid 2 EVRM en artikel 48, lid 1 van het Handvest bepalen dat dat eenieder die wordt beschuldigd van een strafbaar feit geacht wordt onschuldig tot zijn schuld in rechte is komen vast te staan.[766] Deze onschuldpresumptie komt onder druk te staan door algoritme-gedreven vormen van *predictive policing*.[767] Algoritmes kunnen detecteren welke personen waarschijnlijk een strafbaar feit zullen plegen, pogen te plegen, voorbereiden of beramen.[768] *Predictive policing* stelt opsporingsautoriteiten aldus in staat om te voorspellen welke mensen een neiging hebben 'tot geweldpleging, pedofilie, fraude met belastingen of sociale zekerheid of fundamentalistisch radicalisme.'[769] Buruma merkt op dat de kans op

762 Zie de noot van Van Eck bij ABRvS 17 mei 2017, *Computerrecht* 2017/256.
763 Zie hoofdstuk II, par. 5.3.
764 Prakken 2018, p. 271.
765 Zie in dit kader, 'De robotrechter: dit is mijn berekening, en daar moet u het mee doen', *Trouw* 25 november 2017, online via: https://www.trouw.nl/home/de-robotrechter-dit-is-mijn-berekening-en-daar-moet-u-het-mee doen~a25e188e/ (laatst geraadpleegd 4 februari 2018).
766 Zie nader hoofdstuk II, paragraaf 4.3.
767 Zie Wagner 2017, p. 8.
768 Hildebrandt 2016d, p. 194.
769 Buruma 2016.

strafrechtelijke aansprakelijkheid enkel op deze gronden klein is en niet in het verschiet ligt, al is op basis van de strafbaarstelling van voorbereidingshandelen (art. 46 Sr) al veel mogelijk.[770] De kans dat (grondrechtenbeperkende) strafvorderlijke bevoegdheden worden ingezet op basis van *predictive policing*, is echter aanzienlijk groter. Niet alleen krijgt de door Borgers omschreven 'vlucht naar voren' hiermee een nieuwe dimensie,[771] maar ook staat een dergelijke inzet van overheidsmacht op gespannen voet met de onschuldpresumptie.[772]

770 Idem.
771 Borgers 2007.
772 Hildebrandt 2016d, p. 194-195. Zie verder over dit thema Ferguson 2015 en WRR 2016, p. 113. Zie voor een ander perspectief in dit kader Bemelmans 2018, p. 148.

IV Conclusie

In dit laatste hoofdstuk wordt allereerst een samenvattend overzicht gegeven van de in hoofdstuk III benoemde knelpunten. Vervolgens worden deze potentiële negatieve effecten in samenhang bezien en wordt een aanzet gegeven voor het identificeren van de meest urgente grondrechtelijke problemen die zich voordoen als gevolg van de in hoofdstuk I omschreven algoritme-gedreven technologieën.

IV.1 Overzicht van grondrechtelijke knelpunten

IV.1.1 Privacyrechten

Bij de uitoefening van privacyrechten kan een veelheid van grondrechtelijke knelpunten ontstaan als gevolg van de drie besproken technologieën. Dit vindt zijn grondslag in de ruime reikwijdte van deze rechten, in combinatie met het gedetailleerde beeld dat met behulp van algoritme-gedreven technologieën verkregen kan worden van het leven van burgers. De knelpunten die zijn geïdentificeerd bij de uitoefening van privacyrechten kunnen zich voordoen in zowel verticale (overheid-burger) als horizontale (private) verhoudingen en ze worden voornamelijk veroorzaakt door Big Data en het IoT. Meer specifiek kunnen de volgende (potentiële) knelpunten van algoritme-gedreven technologieën worden geïdentificeerd:

– Uit rechtspraak van het EHRM kan worden afgeleid dat surveillance ('dataveillance') door middel van moderne technologieën als Big Data en het IoT een inbreuk kan opleveren op het recht op privacy. Deze inbreuken kunnen zich zowel voordoen in de privéomgeving als in publieke ruimtes, bijvoorbeeld in *smart cities*. Surveillance met behulp van Big Data en het IoT in horizontale rechtsverhoudingen verdient eveneens aandacht. Uit recente EHRM-rechtspraak kan worden afgeleid dat de inzet van het IoT door bedrijven, bijvoorbeeld op de werkvloer, kan raken aan de positieve verplichting tot het vastellen van regelgeving die ziet op het waarborgen van het recht op privacy in dergelijke situaties. Ook in de rechtspraak kan het recht op privacy bij de inzet van Big Data en het IoT in de relaties tussen particulieren een belangrijke rol gaan spelen, in die zin dat de burgerlijke rechter verplicht kan zijn om de EVRM-rechtspraak over privacy te volgen. Daarbij is van belang dat dit soort inbreuken op de privacy steeds moeten voldoen aan de beperkingseisen die door de relevante grondrechtenbepalingen worden gesteld. Daarbij verdient met name de materiële beperkingseis van artikel 8 EVRM aandacht, bijvoorbeeld in het kader van de inzet van politiële datamining en

het gebruik van het IoT ten behoeve van de opsporing. In het bijzonder betekent dit bijvoorbeeld dat regelgeving voldoende duidelijk moet zijn verwoord om de consequenties van het gebruik van bepaalde technologieën te kunnen inschatten, dat voldoende waarborgen moeten worden geboden tegen willekeurig gebruik hiervan, en dat toegang tot rechtsbescherming moet worden geboden.
- Meer algemeen behoeven inbreuken op het recht op privacy door middel van Big Data en het IoT een wettelijke grondslag. Als daarbij gebruik wordt gemaakt van de mogelijkheid van delegatie aan decentrale overheden, dan moet de regeling die in de beperking voorziet voldoende gespecificeerd zijn, dat wil zeggen uitdrukkelijk geschreven voor de beperking van het recht op privacy. Daarbij komt dat een specifieke legaliteitsproblematiek zich voordoet bij artikel 13 Grondwet (vertrouwelijke communicatie), artikel 12 Grondwet (bescherming van het binnentreden van de woning) en artikel 11 (lichamelijke integriteit), waarbij steeds moet worden voorzien in een wettelijke basis die aan de in de Grondwet gestelde eisen voldoet.
- De hiervoor benoemde surveillance kan leiden tot 'chilling effects', waardoor het autonome denken en handelen potentieel wordt geraakt. Daarmee raken Big Data en het IoT direct aan het recht op persoonlijke autonomie als gedefinieerd door het EHRM. Dit punt strekt zich eveneens uit tot de vrijheid van godsdienst (*forum internum*) voor zover burgers zich niet langer vrij voelen het eigen geweten en de eigen godsdienst te bepalen.
- De inzet van KI, bijvoorbeeld in de vorm van robots, kan leiden tot moeilijkheden bij het effectueren van het recht op relationele privacy, met name in het kader van de zorg voor hulpbehoevenden; tegelijkertijd kan robotisering juist ook leiden tot vergroting van de mogelijkheden van contact met de buitenwereld en kan deze daarmee positief bijdragen aan het recht op zelfverwerkelijking.
- De-individualisering als gevolg van besluitvorming op basis van Big Data kan op gespannen voet staan met de grondrechtelijke noties van menselijke waardigheid en persoonlijke autonomie.
- Big Data en KI werpen technologische barrières op bij de uitoefening van het recht om vergeten te worden. Hiermee is ook het recht om de eigen identiteit vorm te geven, als deelnorm van het recht op privacy, in het geding.

IV.1.2 Gelijkheidsrechten

De opkomst van Big Data en het IoT leidt ertoe dat de mogelijkheden tot differentiatie tussen (groepen) personen door de overheid en private instellingen toenemen. Dergelijke differentiatie is vanuit grondrechtelijk perspectief problematisch als die leidt tot ongerechtvaardigd onderscheid. Daarbij verdienen met name datamining en profileertechnieken

aandacht, omdat deze inherent gericht zijn op het maken van onderscheid tussen (groepen) individuen. In dit kader is het van belang dat de neutraliteit van de algoritmes waarmee deze technieken werken veelal schijn is, waardoor al te gemakkelijk besluiten worden gebaseerd op uitkomsten van Big Data-analyses. De twee voornaamste oorzaken van ongelijke behandeling door de inzet van Big Data-technieken bij besluitvorming zijn *bias* in de data en *bias* in de gebruikte algoritmes. Als niet steeds wordt onderzocht of dergelijke *bias* zichtbaar zijn, en/of wordt gevraagd om een uitdrukkelijke rechtvaardiging wanneer dat niet het geval is, doet een ongerechtvaardigde ongelijke behandeling zich al snel voor. Discriminatie door algoritmes kan bovendien niet altijd eenvoudig worden ontdekt vanwege de inherente complexiteit en ondoorzichtigheid van algoritmes.

Meer specifiek doen zich daarom de volgende concrete grondrechtelijke knelpunten voor, die onder meer zijn gerelateerd aan het bewijs van algoritmische discriminatie:

- De ondoorzichtigheid en complexiteit van algoritmes kan maken dat het voor mensen onduidelijk is of sprake is van concrete benadeling en ongerechtvaardigde ongelijke behandeling. Algoritmische discriminatie, die ontstaat door een *bias* in de data en/of in de gebruikte algoritmes, kan niet altijd eenvoudig worden ontdekt en gecontroleerd. Dit bemoeilijkt de zichtbaarheid en het bewijs van ongelijke behandeling.
- Het voorgaande geldt in nog sterkere mate als algoritmische discriminatie intentioneel is gemaskeerd. Dit is problematisch, omdat het onder meer in het strafrecht van belang is of sprake is van opzettelijke discriminatie.
- Bij de toepassing van Big Data-analyse gaat het altijd om een veelheid aan factoren die resulteert in onderscheid tussen (groepen) personen. Dit leidt tot een aantal problemen. Zo hangt de toepasselijkheid van specifieke gelijkebehandelingswetten onder meer af van de gronden waarop onderscheid wordt gemaakt (bijvoorbeeld geslacht of seksuele gerichtheid). Het gegeven dat het altijd om een pluraliteit aan gronden gaat, leidt tot een kwalificatieprobleem voor wat betreft de toepasselijke wetgeving, zoals momenteel overigens ook al het geval is voor intersectioneel of meervoudig onderscheid. Dit is van belang omdat specifieke gelijkebehandelingswetten vaak een hoger of een specifiek beschermingsniveau bieden als het gaat om directe discriminatie dan algemene grondrechtelijke codificaties.
- Dat sprake is van directe discriminatie is vaak moeilijk aan te tonen, juist omdat besluiten gebaseerd zijn op een vele (soms ogenschijnlijk neutrale) gronden. Het kan daardoor lastig zijn om directe discriminatie aan te tonen en te profiteren van het hogere beschermingsniveau van specifieke gelijkebehandelingswetten, vooral als geen inzicht bestaat in de werking van een algoritme.
- Het concept van indirecte discriminatie biedt in de hiervoor omschreven gevallen soms, maar niet altijd, uitkomst. Zo kan indirecte discriminatie alleen worden vastgesteld als discriminerende effecten bij een groot aantal gevallen kunnen worden aangetoond.

Ook hier doen zich bewijstechnische complicaties voor die het voor individuele slachtoffers van een ongelijke behandeling moeilijk kunnen maken om succesvol een beroep te doen op het discriminatieverbod.

IV.1.3 Vrijheidsrechten

Het cluster vrijheidsrechten bestrijkt een breed scala aan rechten, variërend van de vrijheid van meningsuiting en de demonstratievrijheid tot het kiesrecht. De grondrechtelijke knelpunten die in hoofdstuk III zijn geïdentificeerd raken daarbij aan de verplichting van de overheid om zich te onthouden van inbreuken op deze rechten, maar zien ook op positieve verplichtingen van de overheid om de effectieve realisering van vrijheidsrechten te verwezenlijken. Een kort overzicht van deze knelpunten illustreert dit:

- Algoritmes die worden ingezet door sociale media en zoekmachines kunnen leiden tot het ontstaan van 'filterbubbels'. Op hun beurt kunnen deze bubbels de pluriformiteit en diversiteit van informatievoorziening aantasten. Deze gevolgen van algoritmes raken aan het recht op vrijheid van meningsuiting en de vrijheid om informatie te ontvangen. Deze rechten beschermen niet alleen tegen negatief overheidsingrijpen, maar vereisen ook actieve bescherming door diezelfde overheid, onder meer om het pluralisme van de media te beschermen en een goede toegang tot informatie te waarborgen. De vraag of en in hoeverre het ook daadwerkelijk een verantwoordelijkheid is van de staat om op te treden tegen filterbubbels, is in de rechtspraak over de vrije toegang tot informatie echter nog niet beantwoord.
- Algoritmes kunnen worden ingezet ten behoeve van 'private censuur' door sociale media en zoekmachines. Onwelgevallige, verdachte of gevaarlijke content kan worden herkend, waarna het bijvoorbeeld onmogelijk wordt om dit soort content te plaatsen of te downloaden, of waarna een bepaalde content automatisch wordt verwijderd. Aan een dergelijke inperking van de vrijheid van meningsuiting kleven grondrechtelijke risico's. Inperking van vrije meningsuiting op het internet kan noodzakelijk zijn ter bescherming van zwaarwegende belangen, maar algoritmes kunnen fouten en (gelet op het onder IV.1.2 geconstateerde) *bias* bevatten. Bovendien bestaat het risico dat met name controversiële, grove of kunstzinnige uitingen verwijderd zullen worden, omdat zij op de grens liggen tussen wat een algoritme als 'aanvaardbaar' of 'onaanvaardbaar' zal herkennen. De vrijheid van meningsuiting dient echter (vooral) ook ter bescherming van onwelgevallige of choquerende opvattingen. Met name voorafgaande beperkingen van uitingen door algoritmes verdienen bijzondere aandacht, omdat hierbij de mogelijkheid tot vrije meningsuiting het meest direct wordt aangetast; door voorafgaande beperkingen kunnen uitingen immers al worden geblokkeerd nog voordat zij hun publiek bereiken.

- Het gegeven dat vrije meningsuiting in toenemende mate plaatsvindt via private bedrijven als Facebook en Google, noopt tot een veranderende houding van de overheid bij het reguleren van meningsuiting. Er kan sprake zijn van indirecte publieke censuur als de overheid samenwerkt met of dreigt met dwang richting sociale media of zoekmachines om onwelgevallige content te verwijderen. Hierbij treden problemen op als de door deze bedrijven gebruikte algoritmes overmatig gaan censureren. De Grondwet verbiedt voorafgaande beperkingen van de vrijheid van meningsuiting volledig. Bovendien leidt het voorgaande tot grondrechtelijke vragen over de rechtsbasis van dergelijk overheidsingrijpen en de voorzienbaarheid van deze inperkingen.
- Bijzondere grondrechtelijke knelpunten ontstaan als de staat op deze manier inbreuk maakt op de vrijheid van meningsuiting met het doel om inbreuken op de eer en goede naam te voorkomen of om discriminatie tegen te gaan (bijvoorbeeld door haatzaaiende content direct te verwijderen). Deze problematiek van botsende grondrechten is niet nieuw, maar krijgt wel extra impact door de snelheid waarmee uitingen door de moderne technologieën kunnen worden geplaatst en verwijderd.
- Het onder IV.1.1 reeds genoemde 'chilling effect' is een risico bij vrije meningsuiting. Big Data en het IoT kunnen ertoe leiden dat burgers hun mening aanpassen of dat zij bepaalde meningen niet meer (op een bepaalde manier) durven over te brengen. Dat geldt zowel voor uitingen in de offline publieke ruimte, als voor uitingen op sociale media en in huiselijke sfeer.
- Knelpunten bij de uitoefening van het recht op vrijheid van demonstratie zijn sterk verwant aan problemen die zijn besproken bij andere clusters van grondrechten. Zo kan de inzet van Big Data en het IoT bij het inperken van demonstratievrijheid leiden tot privacyrechtelijke knelpunten (zie cluster privacyrechten), kunnen deze technieken leiden tot discriminatie (cluster gelijkheidsrechten) of kunnen ze leiden tot een ondoorzichtig, lastig aanvechtbaar besluitvormingsproces (cluster procedurele rechten, zie hierna).
- Hetzelfde geldt voor de uitoefening van het recht op verenigingsvrijheid. Bij het stellen van voorwaarden aan de oprichting of het verbieden van een vereniging kan de overheid Big Data-analyse inzetten, hetgeen kan leiden tot inbreuken op privacy van individuele (aanstaande) leden en tot moeilijkheden bij het aanvechten van een mede op algoritmes gebaseerde beslissing om een vereniging te verbieden.
- In aanvulling op het voorgaande geldt dat als gevolg van de proliferatie van Big Data-toepassingen, verenigingen in toenemende mate gebruik kunnen maken van Big Data-analyse bij beslissingen over het toelaten van leden. Dergelijke beslissingen zijn, door hun potentiële ondoorzichtigheid, mogelijk lastig aan te vechten.
- De inzet van Big Data kan potentieel verstrekkende gevolgen hebben voor de uitoefening van het actieve kiesrecht. Filterbubbels en private of publieke censuur raken aan de toegang tot diverse, onafhankelijke informatie en aan het recht op vrije meningsuiting

in de context van verkiezingen. Deze rechten worden ook geraakt door het inzetten van algoritme-gedreven bots die het politieke discours beïnvloeden, door de inzet van Big Data tijdens verkiezingscampagnes en door algoritmes van Google of Facebook die bepalen welke informatie tot kiezers komt. Ook kan manipulatie van de informatie die zoekmachines of sociale media aan kiezers laten zien, leiden tot beïnvloeding van het gedrag in het stemhokje, met name wanneer dit op een verkiezingsdag gebeurt.
- Het passieve kiesrecht wordt geraakt als politieke partijen Big Data-analyse gebruiken bij het bepalen van de geschiktheid van potentiële kandidaten (zoals ook het geval is bij de verenigingsvrijheid). Verder kunnen Big Data en het gebruik van algoritmes leiden tot beïnvloeding van de opkomst bij verkiezingen.

IV.1.4 Procedurele rechten

Wanneer Big Data, IoT en KI ten grondslag liggen aan beslissingen die de levens van mensen beïnvloeden, en dergelijke beslissingen in rechte worden aangevochten, kunnen deze technologieën de uitoefening van het recht op een eerlijk proces en op toegang tot een effectief rechtsmiddel beïnvloeden. Daarnaast geldt dat Big Data en KI de rechter kunnen ondersteunen bij zijn oordeelsvorming of in de toekomst de rechter zelfs (gedeeltelijk) kunnen vervangen. Rondom deze twee constateringen doen zich enkele grondrechtelijke knelpunten voor:
- Het recht op toegang tot een effectief rechtsmiddel komt in het geding wanneer algoritmes 'ongemerkt' grondrechteninbreuken veroorzaken of wanneer beslissingen die leiden tot dergelijke inbreuken niet transparant zijn onderbouwd. Zo kan algoritmische profilering leiden tot het opstellen van profielen die verbonden zijn met verdachte gronden als ras of seksuele gerichtheid. Wanneer dergelijke profielen vervolgens ten grondslag worden gelegd aan beslissingen die de handelingsopties van personen beïnvloeden, maar deze personen hier niet van op de hoogte van zijn, komt het recht op toegang tot een effectief rechtsmiddel in het gedrang. Ook als bedrijven of overheden weigeren inzicht te geven in de werking van een algoritme, is een beslissing gebaseerd op dit algoritme lastig aanvechtbaar.
- In de rechtspraak zijn tal van procedurele positieve verplichtingen voor de staat erkend als besluiten worden voorbereid die potentieel invloed kunnen hebben op de uitoefening van grondrechten. Hiertoe behoren verplichtingen tot zorgvuldige, open besluitvorming waarbij de burger voldoende wordt betrokken en waarbij deze voldoende wordt geïnformeerd. De ondoorzichtigheid van algoritme-gedreven besluitvorming kan zowel aan deze transparantie als aan betrokkenheid van de burger afbreuk doen.
- Komt een zaak voor een rechter, dan kan de technologische en contextuele complexiteit van algoritme-gedreven besluitvorming ertoe leiden dat niet voldaan wordt aan de

eisen van een open, eerlijk en evenwichtig proces. Met name kan in de rechterlijke procedure sprake zijn van een ongelijke informatiepositie van procespartijen, bijvoorbeeld doordat één van de partijen wel kennis heeft van de werking van een algoritme en de andere niet. Dit kan leiden tot strijdigheid met het recht op *equality of arms*, een deelrecht van het recht op een eerlijk proces. Dergelijke problemen zijn reeds in Nederlandse rechtspraak aan de orde gekomen. Gebleken is bovendien dat dit soort knelpunten zich kan voordoen in zowel strafrechtelijke, bestuursrechtelijke als civielrechtelijke zaken.

- Als Big Data en KI worden ingezet ter ondersteuning of vervanging van rechterlijke oordeelsvorming, kan dit bevorderlijk zijn voor de neutraliteit en kan dit rechters helpen om tot een goed oordeel te komen. Er kunnen echter ook knelpunten optreden als het gaat om het recht op een onafhankelijke en onpartijdige rechter. Rechters kunnen al te zeer worden gestuurd door de werking van algoritmes, wat vooral problematisch is als de herkomst van deze algoritmes niet helemaal duidelijk is of als er *biases* in de algoritmes blijken te zitten. Het 'black box'-karakter van (slimme) algoritmes kan bovendien leiden tot ondoorzichtige rechterlijke besluitvorming.
- In het verlengde van het voorgaande kan de ondoorzichtigheid van algoritmes leiden tot gebrekkig gemotiveerde oordelen, met name als de werking en de uitkomsten van de toepassing van het algoritme zonder meer worden aangenomen. Dit staat op gespannen voet met het recht op een transparante en draagkrachtige motivering.

IV.2 Grondrechtelijke knelpunten in samenhang bezien

Uit hoofdstuk III blijkt dat een breed palet aan grondrechtelijke knelpunten bestaat als gevolg van Big Data, het IoT en KI. Het bestaan daarvan vindt zijn oorzaak primair in de belangrijke, veelomvattende impact die algoritmes (potentieel) op de levens van mensen kunnen hebben, al dan niet in combinatie met het weinig transparante karakter van deze algoritmes. Daarnaast speelt mee dat de codificaties van de relevante grondrechten een groot toepassingsbereik hebben, waardoor de negatieve gevolgen van algoritmes al snel binnen de reikwijdte van deze grondrechten vallen. Een aantal samenhangen kan worden gevonden tussen de geïdentificeerde problemen waar het gaat om de actoren die grondrechtelijke problemen veroorzaken en de rechtsverhoudingen waarin deze zich manifesteren. Daarnaast kan enige samenhang worden gezien in de manieren waarop knelpunten geadresseerd kunnen worden. Deze onderwerpen worden in het hiernavolgende besproken.

IV.2.1 Relevante actoren en rechtsverhoudingen

Grondrechten dienen primair ter bescherming van de burger tegen de overheid. De inzet van algoritme-gedreven technologieën bij het maken van beleid of het nemen van besluiten kan ertoe leiden dat de overheid inbreuk maakt op grondrechten op een manier die voorheen niet was voorzien. De inzet van deze technologieën ten behoeve van surveillance, veelal in het kader van de opsporing van strafbare feiten, kan bijvoorbeeld potentieel leiden tot aanzienlijke inbreuken op de persoonlijke levenssfeer, het huisrecht en de lichamelijke integriteit van burgers. Als de overheid algoritmes inzet in het veiligheidsdomein of deze gebruikt bij het differentiëren tussen groepen personen in het socialezekerheidsdomein, kan dit leiden tot strijdigheid met het recht op gelijke behandeling. Ook de rol van de overheid bij het reguleren van meningsuiting die plaatsvindt via een private, sterk technologie-gedreven infrastructuur, leidt tot nieuwe grondrechtelijke knelpunten, met name doordat de mogelijkheid van indirecte publieke censuur opdoemt. Aan de inzet van algoritmes bij het inperken van demonstratie- en verenigingsvrijheid zijn vergelijkbare risico's verbonden.

De inzet van Big Data, het IoT en KI beperkt zich echter niet tot de overheid. Met name waar het gaat om vrijheidsrechten als vrijheid van meningsuiting, het recht op toegang tot informatie en het kiesrecht gaat de grondrechtelijke aandacht primair uit naar 'usual suspects' als Facebook, Google, Twitter en Youtube. Ook het handelen van grote private instanties als verzekeraars en banken kan grondrechtelijke implicaties hebben, met name waar het gaat om het recht op gelijke behandeling. Daarnaast is gewezen op de proliferatie van algoritme-gedreven besluitvorming door 'kleinere' private actoren als verenigingen, politieke partijen en kleine bedrijven. De hiervoor omschreven surveillanceproblematiek door Big Data en het IoT strekt zich bovendien uit tot bijvoorbeeld werkgevers die het gedrag van hun werknemers monitoren, terwijl ook gelijkebehandelingsproblemen zich kunnen voordoen in de relatie tussen bedrijven en potentiële sollicitanten. Een dergelijke toenemende invloed van algoritme-gedreven technologieën in verschillende alledaagse, typisch privaatrechtelijke situaties, leidt tot een navenant toenemende relevantie van grondrechten in horizontale verhoudingen.

Dit laat zien dat algoritme-gedreven technologieën kunnen leiden tot grondrechtelijke knelpunten, onafhankelijk van de vraag of het een publieke of private actor is die van deze technologieën gebruik maakt. Vanuit het perspectief van de grondrechtencodificaties is het echter wel degelijk van belang onderscheid te blijven maken tussen de horizontale en verticale rechtsverhoudingen waarin grondrechtenschendingen door algoritmes zich voordoen. Grondrechtelijke knelpunten moeten op verschillende manieren geadresseerd worden, afhankelijk van de vraag door wie een inbreuk wordt veroorzaakt. Daarbij is

bovendien van belang dat in de huidige juridische constellatie, het steeds de staat is die een hoofdrol speelt. Vooral vanuit het EVRM zijn er tal van positieve verplichtingen geformuleerd voor de staat om grondrechteninbreuken te voorkomen of, als ze zich onverhoopt hebben voorgedaan, ze te redresseren. De staat moet bijvoorbeeld regulerend optreden om bepaalde grondrechtenschendingen door natuurlijke personen of rechtspersonen te voorkomen, of de rechter moet ervoor zorgen dat in een civiele procedure recht wordt gedaan aan de grondrechten (zie nader paragraaf IV.2.2).

IV.2.2 Legaliteit, positieve verplichtingen, horizontale werking en rechterlijke toetsing

De rol van de wetgever

Grondrechtenbeperkend overheidshandelen behoeft een wettelijke grondslag. De notie van legaliteit speelt daarmee een belangrijke rol wanneer algoritme-gedreven technologieën worden ingezet door de overheid en wanneer deze inzet leidt tot een inperking van grondrechten. Het wettelijk kader voor de inperking van grondrechten behoeft in het licht van de technologische vooruitgang die wordt bewerkstelligd door Big Data, KI en het IoT, een blijvende kritische blik. Vooral privacyrechten en vrijheidsrechten verdienen hierbij aandacht. Zo kan worden gewezen op de noodzaak van adequate regelgeving die bijvoorbeeld de inzet van politiële datamining reguleert of die een wettelijke grondslag biedt voor de inzet van het IoT bij de opsporing. Datzelfde geldt voor mogelijke inperkingen van het huisrecht of lichamelijke integriteit. Ook indirecte publieke censuur behoeft, mede in het licht van het strenge grondrechtelijke regime waar het gaat om voorafgaande beperkingen van uitingsvrijheid, een adequate wettelijke grondslag.

De rol van het bestuur

Het is echter niet alleen de wetgever die een belangrijke rol speelt bij het adresseren van grondrechtelijke knelpunten. Uit grondrechtenbepalingen vloeien ook belangrijke positieve verplichtingen voort voor het bestuur. Hiervoor is al gewezen op het belang van transparantie in publieke besluitvorming. Algoritmische grondrechtenschendingen moeten kenbaar en transparant zijn en betrokkenen moeten voldoende worden betrokken bij besluiten die hun grondrechten in belangrijke mate raken. Dit is ook van belang voor de aanvechtbaarheid van besluiten gebaseerd op algoritmes en daarmee voor de uitoefening van het recht op een effectief rechtsmiddel en toegang tot de rechter. Daarnaast bestaan er diverse verplichtingen tot adequate handhaving en goed toezicht op de naleving van algemene regelgeving, hetzij in de publieke sfeer, hetzij in de private sfeer.

De rol van de overheid bij regulering van het gedrag van private partijen
Zoals hiervoor al is aangegeven, moeten ook knelpunten in private verhoudingen vaak worden geadresseerd via regelgeving. Ook als de overheid niet zelf door negatief ingrijpen een grondrecht inperkt, kan zij dus nog steeds gehouden zijn tot het ondernemen van actie ter bescherming van het betreffende grondrecht. De mogelijke aanwezigheid van positieve reguleringsverplichtingen is in hoofdstuk II en hoofdstuk III op verschillende momenten aan bod gekomen. Zo is bij de inzet van het IoT en Big Data gewezen op gedetailleerde verplichtingen tot regelgeving als het gaat om private surveillance. Ook bij de bescherming van het huisrecht tegen de invloed van het IoT kunnen dergelijke verplichtingen een rol spelen. Datzelfde geldt voor het realiseren van pluriforme informatievoorziening, vrijheid van godsdienst (*forum externum*) en het waarborgen van het kiesrecht.

Voor zover grondrechten horizontale werking toekomen, kunnen knelpunten worden geadresseerd in juridische procedures tussen private partijen waarin (indirect) een beroep op deze grondrechten wordt gedaan. Bij de bespreking van privacyrechten is hierbij gewezen op surveillance door particulieren en inbreuken op de huisvrede of lichamelijke integriteit door het IoT. Ook het recht op vrijheid van meningsuiting komt een zekere betekenis toe in horizontale geschillen. Dit is bijvoorbeeld relevant bij het prioriteren en filteren van informatie door zoekmachines en sociale media. Daarbij heeft een rechter ook de taak om afwegingen tussen grondrechten te maken, zoals in de situatie waarbij iemand zich beroept op het recht om 'vergeten te worden' tegenover een zoekmachine die informatie toegankelijk maakt. Gezien het toenemende belang van algoritmes in private verhoudingen is het waarschijnlijk dat de horizontale werking van grondrechten als privacy en vrijheid van meningsuiting in de rechtspraak verder wordt ontwikkeld, verfijnd en uitgewerkt.

De rol van de rechter
Rechterlijke toetsing speelt een centrale rol bij het adresseren van grondrechtenschendingen, ook wanneer deze samenhangen met het gebruik van algoritmes, en ongeacht de vraag of ze worden veroorzaakt door de staat of door een particulier. Mogelijke grondrechtelijke problemen zullen zich immers in veel gevallen op het niveau van het individu manifesteren en zullen vervolgens leiden tot concrete juridische geschillen. Dat geldt voor alle in dit onderzoek omschreven clusters van grondrechten. De rechter heeft in dit verband een belangrijke verantwoordelijkheid bij het onderkennen en adresseren van de genoemde knelpunten.

Vanwege deze belangrijke rol van de rechter is het des te belangrijker dat sommige knelpunten zich specifiek voordoen bij de effectuering van grondrechten in juridische procedures. Dat geldt bijvoorbeeld bij het recht op gelijke behandeling, ten aanzien waarvan al is gewezen op de bewijstechnische complicaties die het gebruik van algoritmes oplevert,

alsmede de lastige toetsbaarheid van ongelijke behandeling door algoritmes. Ongelijke behandeling door algoritmes is niet altijd zichtbaar, en (in rechte) lastig aan te tonen, hetgeen direct raakt aan de effectiviteit van het recht op gelijke behandeling. In het licht van de importantie van rechterlijke toetsing, zijn daarnaast de knelpunten van belang die zijn geïdentificeerd bij de bespreking van procedurele rechten. Deze rechten zien immers op het bieden van grondrechtelijke waarborgen bij het aankaarten van onrechtmatigheden, waaronder grondrechtenschendingen. Bijzondere aandacht hierbij verdienen het recht op *equality of arms* en de ongelijke informatiepositie die het gevolg kan zijn van het gebruik van slimme algoritmes. Met het toenemende belang van algoritmes in besluitvorming, zullen problemen rondom de verwezenlijking van dit recht zich in de toekomst nog vaker en indringender voordoen.

IV.2.3 Urgentie van de grondrechtelijke knelpunten

Uit de geïdentificeerde knelpunten blijkt een grote samenhang tussen de verschillende besproken grondrechtenclusters. Een recht als godsdienstvrijheid heeft aspecten die bij privacy passen, maar ook aspecten die bij vrijheidsrechten als de uitingsvrijheid passen; het kiesrecht hangt nauw samen met de vrijheid van meningsuiting en het recht op toegang tot informatie; en het recht op gelijke behandeling kan verband houden met alle andere genoemde grondrechten, bijvoorbeeld als aspirant-leden worden uitgesloten van een vereniging of als de toegang tot de rechter voor bepaalde groepen wordt bemoeilijkt. Deze sterke samenhang, gecombineerd met het gegeven dat de omschreven technologieën continu aan ontwikkeling onderhevig zijn, maakt dat het lastig is om te bepalen welke grondrechten het sterkst worden aangetast als gevolg van Big Data, het IoT en KI. Het gaat steeds om een samenspel van grondrechten in concrete omstandigheden tegen de achtergrond van de toenemende rol van algoritmes in verschillende maatschappelijke domeinen.

Hoogstens kunnen sommige van de benoemde knelpunten vanuit grondrechtelijk oogpunt worden beschouwd als minder urgent. Dat geldt bijvoorbeeld voor de bezwaren gerelateerd aan de-individualisering en aantasting van de individuele autonomie. In de afwezigheid van hard empirisch bewijs van concreet nadeel als gevolg van 'chilling effects', filterbubbels of een inperking van de mogelijkheid om autonoom te denken en te handelen, zijn dergelijke knelpunten voorlopig minder prangend. Andere knelpunten zijn vooral een nieuwe variant van problemen die zich als gevolg van oudere technologieën al hebben gemanifesteerd. Dat geldt bijvoorbeeld voor de privacyrechtelijke uitdagingen als gevolg van surveillance met behulp van (algoritme-gedreven) technologieën. De privacyrechtelijke vraagstukken die zich daarbij voordoen zijn niet heel anders of urgenter dan de vraagstukken die zich

al voordeden bij – bijvoorbeeld – het aftappen van telefoons of het volgen van iemand op straat.

Dit is anders voor de gevonden knelpunten bij gelijkebehandelingsrechten en procedurele rechten voor zover ze verband houden met de inherente kenmerken van Big Data, het IoT en KI. Het gaat dan om het fenomeen dat besluiten worden genomen met behulp van slimme algoritmes, waarbij deze algoritmes ondoorzichtig en potentieel niet-neutraal zijn. De problemen die zijn geïdentificeerd bij de bespreking van het recht op gelijke behandeling vloeien voort uit de classificatie van algoritmes als potentieel niet-neutrale constructen. De mogelijke *biases* van algoritmes leiden ertoe dat, telkens wanneer algoritme-gedreven technologieën worden ingezet, het risico op ongerechtvaardigde ongelijke behandeling aanwezig is. Ongelijke behandeling als gevolg van *biases* in algoritmes komt vervolgens telkens terug bij de andere grondrechten, variërend van de vrijheid van betoging en de menselijke waardigheid tot de vrijheid van meningsuiting en de procedurele rechten. Anders gezegd: de alomtegenwoordigheid van algoritmes leidt tot de alomtegenwoordigheid van mogelijke problemen van ongerechtvaardigde ongelijke behandeling. Vanuit dit perspectief bezien, doen zich bijzonder urgente problemen voor bij de uitoefening van gelijkebehandelingsrechten.

De knelpunten bij procedurele rechten vloeien voornamelijk voort uit de ondoorzichtigheid van slimme algoritmes. Deze ondoorzichtigheid kan ertoe leiden dat het ontbreekt aan goede, transparante en kenbare motivering van (publiekrechtelijke en privaatrechtelijke) beslissingen die zijn gebaseerd op of mede zijn ingegeven door technologisch en contextueel complexe, slimme algoritmes. Hiervoor is al aangegeven dat dit problematisch kan zijn in het licht van het recht op een effectief rechtsmiddel, het recht op toegang tot de rechter en het recht op *equality of arms*. Dat is te meer problematisch nu knelpunten bij de uitoefening van procedurele rechten raken aan de effectiviteit van andere (materiële) grondrechten. Mogelijke schendingen van het recht op privacy, gelijke behandeling, vrijheid van meningsuiting en andere grondrechten moeten immers in rechte kunnen worden aangevochten, in een rechtsgang die aan de eisen van het recht op een eerlijk proces voldoet. Als deze mogelijkheid ontbreekt, juist door het gebruik van algoritmes in besluitvorming of in de rechtspraak, leidt digitalisering niet alleen tot een verhoogd risico van schending van materiële grondrechten, maar komt ook adequate rechtsbescherming tegen dergelijke schendingen onder druk te staan. Om deze redenen verdienen de knelpunten bij de uitoefening van procedurele rechten urgente aandacht.

De twee belangrijkste knelpunten overziend is daarmee met name de vraag hoe bijgedragen kan worden aan het vergroten van de neutraliteit en transparantie van algoritmes. Daarnaast moet urgent antwoord gegeven worden op de vraag hoe de effectiviteit van het recht op

gelijke behandeling en procedurele rechten kan worden gewaarborgd in het licht van *biases* en ondoorzichtigheid van algoritmes. De knelpunten inzake gelijke behandeling en procedurele rechten behoeven daarmee een combinatie van technologische en juridische oplossingen.

IV.2.4 Slotsom

Een eenvoudig antwoord op de onderzoeksvraag is, in het licht van het voorgaande, niet voorhanden – het gaat om een uiterst complexe en veelzijdige materie. In algemene zin geldt niettemin wel dat grondrechten potentieel vergaand en op diverse manieren kunnen worden aangetast als gevolg van het gebruik van het gebruik van Big Data, Kunstmatige Intelligentie en het Internet of Things, vaak ook op manieren die nog niet bekend waren voor 'oude' vormen van besluitvorming. Het voorkomen van dergelijke grondrechtenschendingen en het eventueel bieden van rechtsherstel als ze zich alsnog hebben voorgedaan, verdient dan ook bijzondere aandacht.

Literatuur

AIV 2014
Adviesraad Internationale Vraagstukken, *Het internet: een wereldwijde vrije ruimte met begrensde staatsmacht*, Advies nr. 92, Den Haag 19 december 2014.

AIV 2017
Adviesraad Internationale Vraagstukken, *De wil van het volk. Erosie van de democratische rechtsstaat in Europa*, Advies nr. 104, juni 2017.

Aletras e.a. 2016
N. Aletras, D. Tsarapatsanis, D. Preoțiuc-Pietro & V. Lampos, 'Predicting judicial decisions of the European Court of Human Rights: a Natural Language Processing perspective', *Peer Journal of Computer Science* 2016 2:e93 https://doi.org/10.7717/peerj-cs.93.

Altman 2015
A. Altman, 'Discrimination', in: E.N. Zalta, (red.), *The Stanford Encyclopedia of Philosophy*, interneteditie 2015 (http://plato.stanford.edu/archives/fall2015/entries/discrimination/).

Arnardóttir 2014
O.M. Arnardóttir, 'The Differences that Make a Difference: Recent Developments on the Discrimination Grounds and the Margin of Appreciation under Article 14 of the European Convention on Human Rights', *Human Rights Law Review* 2014, afl. 4, p. 647-670.

Ashton 2009
K. Ashton, 'That 'Internet of Things' Thing', *RFiD Journal* 2009, p. 97-114.

Austin 2006
D. Austin, 'How Google Finds Your Needle in the Web's Haystack' *American Mathematical Society* december 2006, online via: http://www.ams.org/publicoutreach/feature-column/fcarc-pagerank?_sp=9196e030-64b1-48f4-b4f9-5be2ea3f7a31.1515597204154.

Balasubramanian 2015
T. Balasubramanian, 'Social Security and Social Welfare Data Mining: An Overview', *International Journal of Computing Communication and Information System* 2015, afl. 1, p. 15-21.

Balkin 2017
J.M. Balkin, 'Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation' 2017, online via SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3038939.

Barkhuysen e.a. 2018
T. Barkhuysen, M. van Emmerik, O. Jansen & M. Fedorova, 'Right to a fair trial', in: P. van Dijk, F. van Hoof e.a. (red.), *Theory and Practice of the European Convention on Human Rights*, Antwerpen: Intersentia 2018, p. 497-654.

Barkhuysen & Van Emmerik 2013
T. Barkhuysen & M.L. van Emmerik, 'Politieke rechten: kiesrecht en petitierecht', in: J.H. Gerards (red.), *Grondrechten. De nationale, Europese en internationale dimensie*, Nijmegen: Ars Aequi 2013.

Barkhuysen & Van Emmerik 2018
T. Barkhuysen & M.L. van Emmerik, 'Right to an effective remedy', in: P. van Dijk, F. van Hoof e.a. (red.), *Theory and Practice of the European Convention on Human Rights*, Antwerpen: Intersentia 2018, p. 1035-1061.

Barkhuysen, Van Emmerik & Gerards 2013
T. Barkhuysen, M.L. van Emmerik & J.H. Gerards, 'Rechten van bijzondere groepen en collectieve rechten', in: J.H. Gerards e.a. (red.), *Grondrechten. De nationale, Europese en internationale dimensie*, Nijmegen: Ars Aequi Libri 2013.

Barocas & Selbst 2016
S. Barocas & A.D. Selbst, 'Big Data's Disparate Impact', *California Law Review* 2016, afl. 3, p. 671-732.

Bauw 2017
E. Bauw, *Politieke processen. Over de rol van de civiele rechter in de democratische rechtsstaat*, oratie Universiteit Utrecht 2017, Den Haag: Boom juridisch 2017.

Beer 2013
D. Beer, 'Algorithms: Shaping Tastes and Manipulating the Circulations of Popular Culture', in: D. Beer (red.) *Popular Culture and New Media. The Politics of Circulation*, Londen: Palgrave Macmillan 2013, p. 63-100.

Van Beers 2009
B. van Beers, *Persoon en lichaam in het recht* (diss. Amsterdam VU), Den Haag: Boom Juridische Uitgevers 2009.

Beijer 2017
M.P. Beijer, *The Limits of Fundamental Rights Protection by the EU. The Scope for the Development of Positive Obligations* (diss. Nijmegen), Antwerpen: Intersentia 2017.

Bell 2007
M. Bell, 'Direct Discrimination', in: D. Schiek, L. Waddington & M. Bell (red.), *Cases, Materials and Text on National, Supranational and International Non-Discrimination Law*, Oxford: Hart 2007, p. 185-322.

Bemelmans 2018
J.H.B. Bemelmans, *Totdat het tegendeel is bewezen. De onschuldpresumptie in rechtshistorisch, theoretisch, internationaalrechtelijk en Nederlands strafprocesrechtelijk perspectief* (diss. Nijmegen), Deventer: Kluwer 2018.

Bentham 1791
J. Bentham, *The Panopticon Writings* [1791], bewerkt door Miran Božovič, Londen: Verso 1995.

Blok 2017
P.H. Blok (red.), *Big data en het recht: een overzicht van het juridisch kader voor big data-toepassingen in de private sector,* Den Haag: Sdu 2017.

Bond e.a. 2012
R.M. Bond e.a., 'A 61-million-person experiment in social influence and political mobilization', *Nature* 2012 (489), p. 295-298.

Boonk & Lodder 2006
M. Boonk & A.R. Lodder, 'Regulating Website Access for Automated Means Such as Search Bots and Agents: Property or Contract?', *Contemporary Issues in Law* 2005/2006, afl. 4, p. 360 - 374.

Borgers 2007
M.J. Borgers, *De vlucht naar voren* (oratie Amsterdam VU 2007), Den Haag: Boom Juridische uitgevers 2007.

Böstrom e.a. 2007
H. Boström, S.F. Andler, M. Brohede, R. Johansson, A. Karlsson, J. van Laere, L. Niklasson, M. Nilsson, A. Persson & T. Ziemke, *On the Definition of Information Fusion as a Field of Research,* Technical report, University of Skövde, School of Humanities and Informatics, online via: http://www.diva-portal.org/smash/get/diva2:1175340/FULLTEXT01.pdf (laatst geraadpleegd 16 februari 2018).

Bozdag 2013
E. Bozdag, 'Bias in algorithmic filtering and personalization', *Ethics and Information Technology* 2013, afl. 3, p. 209–227.

Bovend'Eert 2013
P.P.T. Bovend'Eert, *Rechterlijke organisatie, rechters en rechtspraak*, Deventer: Kluwer 2013.

Brems & Vrielink 2010
E. Brems & J. Vrielink, *Voorstudie ten behoeve van de Staatscommissie Grondwet*, Deventer: Kluwer, 2010.

Brinkhoff 2016
S. Brinkhoff, 'Big data datamining door de politie: IJkpunten voor een toekomstige opsporingsmethode', *Nederlands Juristenblad* 2016, afl. 20, p. 1401-1407.

Brinkhoff 2017
S. Brinkhoff, 'Datamining in een veranderende wereld van opsporing en vervolging', *Tijdschrift voor Bijzonder Strafrecht en Handhaving* 2017, afl. 4, p. 224-227.

Broeksteeg & Dorssemont 2017
J.L.W. Broeksteeg & F. Dorssemont, 'Artikel 11. Vrijheid van vreedzame vergadering en van vereniging', in: J.H. Gerards e.a. (red.), *Sdu Commentaar EVRM. Deel 1 – Materiële rechten*, online via opmaat.sdu.nl, bijgewerkt tot en met 14 september 2017.

Broeksteeg & Terlouw 2011
J.L.W. Broeksteeg & A.B. Terlouw, *Overheid, recht en religie*, Deventer: Kluwer 2011.

Brouwers & Kummeling 2016
L. Brouwers & H. Kummeling, 'De gelijke toegang tot de rechter onder vuur', in: R. Ortlep e.a. (red.), *De rechter onder vuur*, Oisterwijk: WLP 2016, p. 153-178.

Buisman & Kierkels 2013
S.S. Buisman & S.B.G. Kierkels,' Wetenschappelijk commentaar op artikel 12 Grondwet. Binnentreden woning, december 2013, online via: http://www.nederlandrechtsstaat.nl/grondwet/artikel.html?artikel=12#.

Business Insider 2016
Business Insider, 'Apple just bought new tech that can analyze your emotions — here's how it works', 7 januari 2016, online via: http://www.businessinsider.com/how-emotient-ai-works-2016-1?international=true&r=US&IR=T.

Buruma 2016
Y. Buruma, 'De criminele homo digitalis', *Nederlands Juristenblad* 2016, afl. 22, p. 1534-1541.

Buyse 2016
A.C. Buyse, *Dignified Law: The Role of Human Dignity in European Convention Case-Law*, keynote lecture 11 October 2016, online via: http://echrblog.blogspot.nl/2016/10/the-role-of-human-dignity-in-echr-case.html.

Calders & Custers 2013
T. Calders & B.H.M. Custers, 'What is data mining and how does it work?', in: B.H.M. Custers e.a. (red.), *Discrimination and privacy in the information society*, Heidelberg: Springer 2013, p. 27-42.

Calders & Žliobaitė 2012
T. Calders & I. Žliobaitė, 'Why Unbiased Computational Processes Can Lead to Discriminative Decision Procedures', in: B. Custers, T. Calders, B. Schermer & T. Zarsky, *Discrimination and Privacy in the Information Society*, Springer 2012, p. 43-57.

Castanedo 2013
F. Castanedo, 'A Review of Data Fusion Techniques', *The Scientific World Journal* 2013, afl. 19 online via: https://www.hindawi.com/journals/tswj/2013/704504/.

Castelvechhi 2016
D. Castelvechhi, 'Can we open the black box of AI?', *Nature* 2016, afl. 5, p. 20-23.

Centraal Planbureau 2017
Centraal Planbureau, 'Scientia potentia est: de makelaar van alles', *CPB Policy Brief* 2017/11, 15 december 2017.

Cerka, Grigiene & Sirbikytels 2017
P. Cerka, J. Grigiene & G. SirbikyteIs, 'Is it possible to grant legal personality to artificial intelligence software systems?', *Computer law & security review* 2017, afl. 5, p. 685-699.

Citron & Pasquale 2014
D.K. Citron & F. Pasquale, 'The Scored Society: Due Process for Automated Predictions', *Washington Law Review* 2014, afl. 1, p. 1-33.

Colonna 2013
L. Colonna, 'A Taxonomy and Classification of Data Mining', *SMU Science & Technology Law Review* 2013, p. 309-369.

Commissie Grondrechten in het digitale tijdperk 2000
Commissie Grondrechten in het digitale tijdperk, *Rapport Commissie Grondrechten in het digitale tijdperk*, Den Haag 2000.

Commissariaat voor de Media 2017
Commissariaat voor de Media, *15 jaar Mediamonitor. Van mediaconcentratie naar mediagebruik*, juni 2017.

Commissie-Wolfsen 2015
Commissie onderzoek oorzaken kostenstijgingen stelsel gesubsidieerde rechtsbijstand en vernieuwing van het stelsel (Commissie-Wolfsen), *Herijking rechtsbijstand. Naar een duurzaam stelsel voor de gesubsidieerde rechtsbijstand*, Den Haag 2015.

Cornet e.a. 2016
L.J.M. Cornet, F. Bootsman, D.L. Alberda & C.H. de Kogel, *Neurowetenschappelijke toepassingen in de jeugdstrafrechtketen. Inventarisatie instrumenten, preventie en interventie*, Den Haag: WODC 2016.

Coster van Voorhout 2017
J.E.B. Coster van Voorhout, 'C.13 Rechtsbijstand', in: J.H. Gerards e.a. (red.), *Sdu Commentaar EVRM. Deel I – materiële rechten*, online via opmaat.sdu.nl, bijgewerkt tot en met 15 juni 2017.

Council of Europe 1979
Council of Europe, *Collected Texts*, Straatsburg 1979.

Covington, Adams & Sargin 2016
P. Covington, J. Adams & E. Sargin, 'Deep Neural Networks for YouTube Recommendations', *Proceedings of the 10th ACM Conference on Recommender Systems* 2016, online via: https://research.google.com/pubs/pub45530.html.

Crovitz 2012
L.G. Crovitz, 'Obama's "Big Data" Victory', *Wall Street Journal* 18 november 2012, online via: https://www.wsj.com/articles/SB10001424127887323353204578126671124151266.

Custers 2013
B.H.M. Custers, 'Data Dilemmas in the Information Society', in: B.H.M. Custers e.a. (red.) *Discrimination and Privacy in the Information Society*, Heidelberg: Springer, p. 3-26.

Custers 2017
B.H.M. Custers, 'Big data en big data technologie', in: P.H. Blok (red.), *Big data en het recht: een overzicht van het juridisch kader voor big data-toepassingen in de private sector*, Den Haag: Sdu 2017, p. 17-35.

Dalenberg 2017
D.J. Dalenberg, 'Preventing discrimination in the automated targeting of job advertisements', *Computer Law & Security Review* 2017, p. 1-13.

Diakopoulos 2015
N. Diakopoulos, 'Algorithmic Accountability', *Digital Journalism* 2015, afl. 3, p. 398-415.

Van Dijk & Van Hoof 1998
P. van Dijk & G.J.H. van Hoof 1998*, Theory and Practice of the European Convention on Human Rights*, Den Haag: Kluwer Law International 1998.

Dijkstra e.a. 2016
M. Dijkstra, S. Joosten, E. Stamhuis & M. Visser, 'Beginselen digitaal. Digitalisering en de beginselen van de strafrechtspleging, Den Haag: WODC 2016.

Dubelaar 2017
M.J. Dubelaar, 'C.14 Oproepen en ondervragen van getuigen', in: J.H. Gerards e.a. (red.), *Sdu Commentaar EVRM. Deel I – materiële rechten*, online via opmaat.sdu.nl, bijgewerkt tot en met 15 juni 2017.

Dutch Data Center Association 2017
Dutch Data Center Association, *Internet of Things*, 6 juni 2017 p.1, online via: https://www.dutchdatacenters.nl/dda-publiceert-rapport-toepassing-en-impact-internet-things/.

Economist 2015
'Augmented business', *The Economist* 4 november 2010, via: http://www.economist.com/node/17388392.

Van den Eijnden 2011
P.M. van den Eijnden, *Onafhankelijkheid van de rechter in constitutioneel perspectief* (diss. Nijmegen), Deventer: Kluwer 2011.

Van den Eijnden 2017
P.M. van den Eijnden, 'C.8 Onafhankelijk en onpartijdig gerecht', in: J.H. Gerards e.a. (red.), *Sdu Commentaar EVRM. Deel I – materiële rechten*, online via opmaat.sdu.nl, bijgewerkt tot en met 15 juni 2017.

Epstein 2015
R. Epstein, 'How Google Could Rig the 2016 Election', via: https://www.politico.com/magazine/story/2015/08/how-google-could-rig-the-2016-election-121548?o=0.

Epstein & Robertson 2015
R. Epstein & R.E. Robertson, 'The search engine manipulation effect (SEME) and its possible impact on the outcomes of elections', *Proceedings of the National Academy of Sciences* 2015, afl. 33, p. E4512-E4521.

Epstein e.a. 2017
R. Epstein e.a., 'Suppressing the Search Engine Manipulation Effect (SEME)', *Proceedings of the ACM on Human-Computer Interaction* 2017, afl. 1, p. 42:1-42:23.

Van Est & Gerritsen 2017
R. van Est & J. Gerristen (m.m.v. L. Kool), *Human rights in the robot age Challenges arising from the use of robotics, artificial intelligence, and virtual and augmented reality*, Den Haag: Rathenau Instituut 2017.

Van Ettekoven & Marseille 2017
B.J. van Ettekoven & A.T. Marseille, 'Afscheid van de klassieke procedure in het bestuursrecht?', in: L. Coenraad, P. Ingelse, B.J. van Ettekoven, A.T. Marseille, J.H. Crijns

& R.S.B. Kool, *Afscheid van de klassieke procedure: preadviezen*, Handelingen NJV 2017, Deventer: Kluwer 2017, p. 139-264.

European Research Cluster on the Internet of Things 2015
European Research Cluster on the Internet of Things, *Internet of Things – IoT Governance, Privacy and Security Issues*, januari 2015, online via: http://www.internet-of-things-research.eu/pdf/IERC_Position_Paper_IoT_Governance_Privacy_Security_Final.pdf.

Evans 2001
C. Evans, *Freedom of Religion under the European Convention of Human Rights*, Oxford: Oxford University Press 2001.

Evans 2011
D. Evans, *The Internet of Things. How the Next Evolution of the Internet Is Changing Everything*, Cisco White Paper 2011, online via: https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf.

Evers 2016
G.H. Evers, 'In de schaduw van de rechtsstaat: profilering en nudging door de overheid', *Computerrecht* 2016/84, afl. 3, p. 167-171.

Fan & Wu 2011
M. Fan & G. Wu 'Aspect Opinion Mining on Customer Reviews', *Proceedings of the 2011 International Conference on Informatics, Cybernetics, and Computer Engineering (ICCE2011)* 2011, p. 27-33.

Fayyad, Piatetsky-Shapiro & Smyth 1996
U. Fayyad, G. Piatetsky-Shapiro & P. Smyth, 'From data mining to knowledge discovery in databases', *AI Magazine* 1996, afl. 3, p. 37-54.

Ferguson 2015
A.G. Ferguson, A.G., 'Big Data and Predictive Reasonable Suspicion', *University of Pennsylvania Law Review* 2015, afl. 2, p. 327-410.

Forder 2015
C. Forder, 'Artikel 8. Gezinsleven (omgangsrecht, ouderlijke macht, erfrecht, kinderontvoering)', in: J.H. Gerards e.a. (red.), *Sdu Commentaar EVRM. Deel I – materiële rechten*, online via opmaat.sdu.nl, bijgewerkt tot en met 15 juni 2015.

Furnas 2012
A. Furnas, 'Everything You Wanted to Know About Data Mining but Were Afraid to Ask', *The Atlantic* 3 april 2012, online via: https://www.theatlantic.com/technology/archive/2012/04/everything-you-wanted-to-know-about-data-mining-but-were-afraid-to-ask/255388/.

Galetta & De Hert 2014
A. Galetta, A. & P. de Hert, 'Complementing the Surveillance Law Principles of the ECtHR with Its Environmental Law Principles: An Integrated Technology Approach to a Human Rights Framework for Surveillance', *Utrecht Law Review* 2014, afl. 1, p. 55-75.

Gandomi & Haider 2015
A. Gandomi & M. Haider, 'Beyond the hype: Big data concepts, methods and analytics', *International Journal of Information Management* 2015, p. 137-144.

Gartner 2017
Gartner, 'Gartner Says 8.4 Billion Connected "Things" Will Be in Use in 2017. Up 31 Percent From 2016', online via: https://www.gartner.com/newsroom/id/3598917.

Gerards 2002
J.H. Gerards, *Rechterlijke toetsing aan het gelijkheidsbeginsel. Een rechtsvergelijkend onderzoek naar een algemeen toetsingsmodel* (diss. Maastricht), Den Haag: Sdu 2002.

Gerards 2007
J.H. Gerards, 'Grounds of Discrimination', in: M. Bell & D. Schiek (red.), *Cases, Materials and Text on National, Supranational and International Non-Discrimination Law*, Oxford: Hart Publishing 2007, p. 33-184.

Gerards 2008
J.H. Gerards, 'Gronden van discriminatie – de wenselijkheid van open en gesloten opsommingen', in: C. Bayart, S. Sottiaux & S. Van Drooghenbroeck (red.), *De nieuwe federale antidiscriminatiewetten – Les nouvelles lois luttant contre la discrimination*, Brugge: Die Keure/La Charte 2008, p. 129-170.

Gerards 2011
J.H. Gerards, 'Nieuwe ronde, nieuwe kansen: naar een 'semi-open' systeem van gelijkebehandelingswetgeving?', *Nederlands Tijdschrift voor de Mensenrechten | NJCM-Bulletin* 2011, afl. 36-2, p. 144-158.

Gerards 2011b
J.H. Gerards, *EVRM – Algemene beginselen*, Den Haag: Sdu 2011.

Gerards 2011c
J.H. Gerards, 'Pluralism, Deference and the Margin of Appreciation Doctrine', 17 *European Law Journal* 2011 afl. 1, p. 80-120.

Gerards 2014
J.H. Gerards, 'Inadmissibility decisions by the European Court of Human Rights – A critique of the lack of reasoning', *Human Rights Law Review* 2014, afl. 1, p. 148-158.

Gerards 2015
J.H. Gerards 'De EHRM-rechtspraak als richtsnoer bij het opstellen van wetgeving. Enkele relativerende opmerkingen aan de hand van de wetsvoorstellen over gedwongen zorg', *Nederlands Tijdschrift voor Mensenrechten | NJCM-Bulletin* 2015, afl. 3, p. 296-315.

Gerards 2016
J.H. Gerards, 'Artikel 1 Grondwet – Goede gronden voor wijziging?', *Nederlands Tijdschrift voor Mensenrechten | NJCM-Bulletin* 2016, afl. 3, p. 304-318.

Gerards 2017a
J.H. Gerards, 'The Margin of Appreciation Doctrine, the Very Weighty Reasons Test and Grounds of Discrimination', in: M. Balboni (red.), *The principle of discrimination and the European Convention of Human Rights*, Napels: Editoriale Scientifica 2017.

Gerards 2017b
J.H. Gerards, 'Artikel 14. Gelijke behandeling en non-discriminatie', in: J.H. Gerards e.a. (red.), *Sdu Commentaar EVRM*, online via opmaat.sdu.nl, bijgewerkt tot en met juni 2017.

Gerards 2017c
J.H. Gerards, 'Artikel 10. Vrijheid van meningsuiting', in: J.H. Gerards e.a. (red.), *Sdu Commentaar EVRM. Deel 1 – Materiële rechten*, online via opmaat.sdu.nl, bijgewerkt tot en met 15 juni 2017.

Gerards 2017d
J.H. Gerards, *Grondrechten onder spanning. Bescherming van fundamentele rechten in een complexe samenleving*, oratie Universiteit Utrecht 2017.

Gerards, Barkhuysen & Van Emmerik 2014
J.H. Gerards, T. Barkhuysen & M.L. van Emmerik, 'De invloed van de Europese fundamentele rechten op het bestuursrecht', in: B.J. Schueler (red.), *Europeanisering van het algemeen bestuursrecht*, Deventer: Kluwer 2014, p. 33-56.

Gerards, Koffeman & Hendriks 2013
J.H. Gerards, N.R. Koffeman & A.C. Hendriks, 'Zelfbeschikking in het recht van de Raad van Europa, de EU en Nederland', in: *Achtergrondstudies Zelfbeschikking in de Zorg*, Den Haag: ZonMW 2013.

Gill 2017
J.K. Gill, 'Log Analytics With Deep Learning And Machine Learning', 28 april 2017 online via: https://www.xenonstack.com/blog/data-science/log-analytics-with-deep-learning-and-machine-learning.

Gillespie 2014
T. Gillespie, 'The Relevance of Algorithms', in: T. Gillespie, P. J. Boczkowski & K. A. Foot (red.), *Media technologies*: *Essays on communication, materiality, and society*, Cambridge: MIT Press 2014, p. 167-194.

Goedertier & Haeck 2004
G. Goedertier & Y. Haeck, Y., 'Artikel 3 Eerste Protocol – Recht op vrije en geheime verkiezingen', in: J. Vande Lanotte & Y. Haeck (red.), *Handboek EVRM, Deel 2 – Artikelsgewijze Commentaar*, Volume II, Antwerpen/Oxford: Intersentia 2004.

Government Office for Science 2016
Government Office for Science, *Artificial Intelligence: opportunities and implications for future decisionmaking*, 9 november 2016, online via: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/566075/gs-16-19-artificial-intelligence-ai-report.pdf.

Grasseger & Krogerus 2017
H. Grasseger & M. Krogerus, 'The Data that turned the world upside down', via: https://motherboard.vice.com/en_us/article/mg9vvn/how-our-likes-helped-trump-win.

Greer, Gerards & Slowe 2018
S. Greer, J.H. Gerards & R. Slowe, *Human rights in the Council of Europe and the European Union: Achievements, Trends and Challenges*, Cambridge: Cambridge University Press 2018.

Griffin 2016
A. Griffin, 'How Facebook is manipulating you to vote', *The Independent* 5 mei 2016, http://www.independent.co.uk/life-style/gadgets-and-tech/news/uk-elections-2016-how-facebook-is-manipulating-you-to-vote-a7015196.html.

Grimmelmann 2009
J. Grimmelmann, 'The Google Dilemma', *New York Law School Law Review* 2009, p. 939-950.

Hand, Mannila & Smyth 2001
D. Hand, H, Mannila & P. Smyth, *Principles of Data Mining*, Cambridge MAS: MIT Press 2001.

Hardy & Maurushat 2017
K. Hardy & A. Maurushat, 'Opening up government data for Big Data analysis and public benefit, *Computer Law & Security Review* 2017, afl.1, p. 30-37.

Harris e.a. 2014
D. Harris, M. O'Boyle, E. Bates & C. Buckley, *Law of the European Convention on Human Rights*, Oxford: Oxford University Press 2014, p. 555-557.

Hartendorp 2014
R.C. Hartendorp, 'E-Court een goed initiatief dat zich op de verkeerde punten onderscheidt', *Rechtsgeleerd Magazijn Themis*, 2014, afl. 3, p. 117-121.

Van den Heede 2015
P.J.W. van den Heede, 'Artikel 9. Godsdienstvrijheid', in: J.H. Gerards e.a. (red.), *Sdu Commentaar EVRM. Deel 1 – Materiële rechten*, online OpMaat, bijgewerkt tot en met 15 juni 2015.

Helbing e.a. 2017
D. Helbing, B.S. Frey, G. Gigerenzer, E. Hafen, M. Hagner, Y. Hofstetter, J. van den Hoven, R. V. Zicari & A. Zwitter, *Will Democracy Survive Big Data and Artificial Intelligence?*, online via: https://www.scientificamerican.com/article/will-democracy-survive-big-data-and-artificial-intelligence/ .

Van den Herik 1991
J. van den Herik, *Kunnen computers rechtspreken?*, oratie Tilburg 1991.

Heringa 1999
A.W. Heringa, 'Standards of Review for Discrimination. The Scope of Review by the Courts', in: T. Loenen & P. Rodrigues (red.), *Non-Discrimination Law: Comparative Perspectives*, Den Haag/Boston/Londen: Kluwer Law International 1999, p. 27 e.v.

De Hert & Colette 2017
P. De Hert & M. Colette, 'C.10. Onschuldpresumptie', in: J.H. Gerards e.a. (red.), *Sdu Commentaar EVRM. Deel I – materiële rechten*, online via opmaat.sdu.nl, bijgewerkt tot en met 15 juni 2017.

De Hert & Lammerant 2016
P. de Hert & H. Lammerant, 'Predictive Profiling and its Legal Limits: Effectiveness Gone Forever?', in: B. van der Sloot, D. Broeders & E. Schrijvers (red.), *Exploring the Boundaries of Big Data*, Den Haag: WRR 2016.

De Hert, Lammerant & Blok 2017
P. de Hert, H. Lammerant & P.H. Blok, 'Big data en gelijke behandeling', in: P.H. Blok (red.), *Big data en het recht: een overzicht van het juridisch kader voor big data-toepassingen in de private sector*, Den Haag: Sdu 2017, p. 115-134.

Hildebrandt 2006
M. Hildebrandt, 'Profiling: from data to knowledge. Challenges of a crucial technology', *Datenschutz und Datensicherheit* 2006, afl. 9, p. 548-552.

Hildebrandt 2008
M. Hildebrandt, 'Defining Profiling. A New Type of Knowledge?', in: M. Hildebrandt & S. Gutwirth (red.), *Profiling the European Citizen: Cross-Disciplinary Perspectives*, Springer 2008, p. 17-45.

Hildebrandt 2010
M. Hildebrandt, 'Privacy en identiteit in slimme omgevingen', *Computerrecht* 2010/172, afl. 6, p. 273-282.

Hildebrandt 2015
M. Hildebrandt, *Smart Technologies and the End(s) of Law. Novel Entanglements of Law and Technology* 2015, Cheltenham VK: Edward Elgar Publishing 2015.

Hildebrandt 2016a
M. Hildebrandt. 'Datagedreven Onderwijs: Wijs of Onwijs', *Studium Generale Universiteit Utrecht* 2016, online via: https://www.setup.nl/magazine/2016/09/privacyrede-2016.

Hildebrandt 2016b
M. Hildebrandt, 'Learning as a Machine: Crossovers between Humans and Machines', *Journal of Learning Analytics* 2016, afl. 1, p. 6-23.

Hildebrandt 2016c
M. Hildebrandt, 'The New Imbroglio. Living with Machine Algorithms, in: L. Janssens, *The Art of Ethics in the Information Society*, Amsterdam: Amsterdam University Press 2016, p. 55-60.

Hildebrandt 2016d
M. Hildebrandt, 'Data-gestuurde intelligentie in het strafrecht', in: E.M.L. Moerel, J.E.J. Prins, M. Hildebrandt, T.F.E Tjong Tjin Tai, G-J. Zwenne & A.H.J. Schmidt, *Homo Digitalis*, Handelingen NJV 2016, Deventer: Kluwer 2016, p. 137-240.

Van Hoboken 2012
J.V.J. van Hoboken, *Search engine freedom: on the implications of the right to freedom of expression for the legal governance of Web search engines*, Alphen a/d Rijn: Kluwer Law International 2012.

Hoffmann 2014
H.Ch. Hoffmann, 'Article 47 – Right to an Effective Remedy. Specific Provisions (Meaning)', in: S. Peers e.a. (red.), *The EU Charter of Fundamental Rights. A Commentary*, Oxford/Portland: Hart 2014.

Holopainen 2014
L. Holopainen, 'Article 47 – Right to an Effective Remedy. Article 47 (3): Legal aid shall be made available to those who lack sufficient resources in so far as such aid is necessary to ensure effective access to justice', in: S. Peers e.a. (red.), *The EU Charter of Fundamental Rights. A Commentary*, Oxford/Portland: Hart 2014, p. 1269-1272.

Holtmaat 2003
R. Holtmaat, 'Stop de inflatie van het discriminatiebegrip! Een pleidooi voor het maken van onderscheid tussen discriminatie en ongelijke behandeling', *Nederlands Juristenblad* 2003, p. 1265.

Holtmaat 2006
R. Holtmaat, 'Discriminatie of onderscheid: het kleine verschil met grote gevolgen of het grote verschil met kleine gevolgen?', in: M.L.M. Hertogh & P.J.J. Zoontjens, *Gelijke behandeling: principes en praktijken. Evaluatieonderzoek Algemene wet gelijke behandeling*, Nijmegen: WLP 2006, p. 1-113.

Human Rights Committee 1988
Human Rights Committee, *CCPR General Comment No. 16: The right to respect of privacy, family, home and correspondence, and protection of honour and reputation* (*Art. 17*), 8 april 1988.

Human Rights Watch 2012
Human Rights Watch, 'Losing Humanity. The Case against Killer Robots', 19 november 2012, online via: https://www.hrw.org/report/2012/11/19/losing-humanity/case-against-killer-robots.

Van Hout 2017
M.B.A. van Hout, 'Rechtsbescherming in het tijdperk van big data', *Weekblad fiscaal recht* 2017/165, p. 1036-1046.

Van den Hoven van Genderen 2017
R. van den Hoven van Genderen, 'Privacy and Data Protection in the Age of Pervasive Technologies in AI and Robotics', *European Data Protection Law Review* 2017, afl. 3, p. 1-15.

Hurley & Adebayo 2016
M.A Hurley & J. Adebayo, 'Credit Scoring in the Era of Big Data', *Yale Journal of Law & Technology* 2016, p. 148-216.

International Data Corporation 2017
International Data Corporation, *White Paper - Data Age 2025: The Evolution of Data to Life-Critical*, April 2017, online via:https://www.seagate.com/files/www-content/our-story/trends/files/Seagate-WP-DataAge2025-March-2017.pdf.

Issenberg 2012
S. Issenberg, *The Victory Lab. The Secret Science of Winning Campaigns*, New York: Crown 2012.

International Telecommunication Union 2005
International Telecommunication Union, *The Internet of Things*, november 2005, online via: https://www.itu.int/net/wsis/tunis/newsroom/stats/The-Internet-of-Things-2005.pdf.

International Telecommunication Union 2012
International Telecommunication Union, *Overview of the Internet of Things*, 15 juni 2012, http://www.itu.int/ITU-Y/recommendations/rec.aspx?rec=Y.2060.

The Internet Architecture Board 2015
The Internet Architecture Board, 'RFC 7452. Architectural Considerations in Smart Object Networking' maart 2015), https://tools.ietf.org/html/rfc7452.

The Internet Society 2015
The Internet Society, *The Internet of Things: an overview. Understanding the Issues and Challenges of a More Connected World*, oktober 2015, online via: https://www.internetsociety.org/resources/doc/2015/iot-overview.

Janssen 2003
H.L. Janssen, *Constitutionele interpretatie. Een rechtsvergelijkend onderzoek naar de vaststelling van de reikwijdte van het recht op persoonlijkheid* (diss. Maastricht 2003), Den Haag: Sdu 2003.

De Jong 2017
T. de Jong, *Procedurele waarborgen in materiële EVRM-rechten* (diss. Leiden 2017).

Jongbloed 2014
A.W. Jongbloed, 'E-Court; een miskend initiatief om de kosten voor procederende burgers acceptabel te houden'. *Rechtsgeleerd Magazijn Themis* 2014, afl. 3, p. 111-117.

Joseph, Schultz & Castan 2004
S. Joseph, J. Schultz & M. Castan, *The International Covenant on Civil and Political Rights Cases, Materials and Commentary*, Oxford: Oxford University Press 2004.

Kemp 2014
R. Kemp, 'Legal aspects of managing Big Data', *Computer Law & Security Review*, afl. 5, p. 482-491.

King & Forder
N.J. King & J. Forder, 'Data analytics and consumer profiling: Finding appropriate privacy principles for discovered data', *Computer Law & Security Review*, afl. 5, p. 696-714.

Kitchin 2014
R. Kitchin, *The Data Revolution: Big Data, Open Data, Data Infrastructures and their Consequences*, London: Sage 2014.

Kitchin & McArdle 2016
R. Kitchin & G. McArdle, 'What makes Big Data, Big Data? Exploring the ontological characteristics of 26 datasets', *Big Data & Society* 2016, p. 1-10.

Klonick 2018
K. Klonick, 'The New Governors: The People, Rules, and Processes Governing Online Speech', 131 *Harvard Law Review* 2018 (te verschijnen), online beschikbaar via SSRN: https://ssrn.com/abstract=2937985.

Koffeman 2015
N.R. Koffeman, 'Artikel 8. Privéleven: autonomie en menselijke waardigheid, fysieke integriteit, abortus en euthanasie, ivf-behandelingen, informed consent', in: J.H. Gerards e.a. (red.), *Sdu Commentaar EVRM. Deel I – materiële rechten*, online via opmaat.sdu.nl, bijgewerkt tot en met 15 juni 2015.

Kollanyi, Howard & Woolley 2016
B. Kollanyi, P.N. Howard & S.C. Woolley, 'Bots and Automation over Twitter during the First U.S. Presidential Debate', in: *Computational Propaganda Data Memo* 2016, afl. 4, p. 1-4.

De Koning 2016
M. de Koning, 'Fair play en marktwerking in de privacygevoelige wereld van Big Data', *Computerrecht* 2016/83, afl. 3, p. 160-166.

Kortmann 2012
C.A.J.M. Kortmann, *Constitutioneel recht*, Deventer: Kluwer 2012.

Kool e.a. 2017
L. Kool, J. Timmer, L. Royakkers & R. van Est, *Opwaarderen. Borgen van publieke waarden in de digitale samenleving*, Den Haag: Rathenau Instituut 2017.

Koops 2009
B.J. Koops, 'Over 'mensen' en 'mensen'-rechten. De maakbare mens bezien vanuit het perspectief van grondrechten', in: B.J. Koops e.a., *De maakbare mens. Tussen fictie en fascinatie*, Amsterdam: Bert Bakker 2009.

Koops e.a. 2012
B.J. Koops, G. Bodea, G. Broenink, C. Cuijpers, L. Kool, C. Prins & M. Schellekens, *Juridische scan openbrononderzoek. Een analyse op hoofdlijnen van de juridische aspecten van de iRN/iColumbo-infrastructuur en HDIeF-tools*, Tilburg: TILT 2012.

Koops e.a. 2013
B.J. Koops, A. Di Carlo, L. Nocco, V. Cassamassima & E. Stradella, 'Robotic technologies and fundamental rights: Robotics challenging the European constitutional framework', *International Journal of Technoethics* 2013, afl. 2, p. 15-35.

Koops e.a. 2017
B.J. Koops e.a., 'A Typology of Privacy', 38 *University of Pennsylvania International Law Review* 2017, afl. 2, p. 483-575.

Koops & Cuijpers 2009
B.J. Koops & C. Cuijpers, 'Begluren en besturen door slimme energiemeters: een ongerechtvaardigde inbreuk op onze privacy', 12 *Privacy & Informatie* 2009, afl. 1, p. 3-8.

Koops & Prinsen 2007
B.J. Koops & M.M. Prinsen, 'Houses of glass, transparent bodies: How new technologies affect inviolability of the home and bodily integrity in the Dutch constitution', *Information & Communications Technology Law* 2007, afl. 3, p. 177-190.

Korenhof & Koops 2013
P. Korenhof & E.J. Koops, 'Gender Identity and Privacy: Could a Right To Be Forgotten Help Andrew Agnes Online?', *TILT Law & Technology Working Paper* No. 3/2013, online via SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2304190.

Kosinskia, Stillwella & Graepel 2012
M.Kosinskia, D. Stillwella & T. Graepel, 'Private traits and attributes are predictable from digital records of human behavior', *Proceedings of the National Academy of Sciences (PNAS),* online via: www.pnas.org/content/early/2013/03/06/1218772110.

Kramer, Guillory & Hancock 2014
A.D. Kramer, J.E. Guillory & J.T. Hancock, 'Experimental evidence of massive-scale emotional contagion through social networks', *Proceedings of the National Academy of Sciences* 2014, afl. 24, p. 8788-8790.

Kranzberg 1986
M. Kranzberg, 'Technology and History: 'Kranzberg's Laws', *Technology and Culture* 1986, afl. 3, p. 544-560.

Kroll e.a. 2017
J.A. Kroll, S. Barocas, E.W. Felten, J.R. Reidenberg, D.G. Robinson & H. Yu, 'Accountable Algorithms', *University of Pennsylvania Law Review* 2017, afl. 3, p. 633-705.

Labrinidis & Jagadish 2012
A. Labrinidis & H.V. Jagadish, 'Challenges and opportunities with big data, *Proceedings of the VLDB Endowment* 2012, afl. 12, p. 2032-2033.

Lafarre 2016
A. Lafarre, 'Recht voor big data, big data voor recht', *Computerrecht* 2016/80, afl. 3, p. 146-149.

Laitinen, Niemelä & Pirhonen 2016
A. Laitinen, M. Niemelä & J. Pirhonen, 'Social Robotics, Elderly Care, and Human Dignity: A Recognition-Theoretical Approach', in: J. Seibt (red.) *What Social Robots Can and Should*, IOS Press 2016.

Landelijke Organisatie Sociaal Raadslieden 2018
Landelijke Organisatie Sociaal Raadslieden, *Rechtspraak op bestelling?! Stop commerciële rechtspraak*, 17 april 2018, via: https://www.sociaalwerknederland.nl/thema/sociaal-raadsliedenwerk-srw/nieuws/6112-analyse-en-aanbevelingen-rond-commerciele-rechtspraak.

Laney 2001
D. Laney, '3D data management: Controlling data volume, velocity and variety', online via: http://blogs.gartner.com/doug-laney/files/2012/01/ad949-3D-Data-Management-Controlling-Data-Volume-Velocity-andVariety.pdf.

Lavrysen 2016
L. Lavrysen, *Human Rights in a Positive State. Rethinking the Relationship between Positive and Negative Obligations under the European Convention on Human Rights*, Antwerpen: Intersentia 2016.

Lee 2016
C. Lee, *Big Data in Management Research: Exploring New Avenues* (diss. Rotterdam 2016), Rotterdam: Erasmus University 2016.

Leeuw 2013
B.J.G. Leeuw, *Grondwet en eerlijk proces. Een onderzoek naar de eventuele meerwaarde van het opnemen van het recht op een eerlijk proces in de Nederlandse Grondwet* (diss. Rotterdam 2013), Oisterwijk: WLP 2013.

Leeuw 2017
B.J.G. Leeuw, 'C.1. Toegang tot de rechter', in: J.H. Gerards e.a. (red.), *Sdu Commentaar EVRM. Deel I – materiële rechten*, online via opmaat.sdu.nl, bijgewerkt tot en met 15 juni 2017.

Leijten 2015
A.E.M Leijten, *Core rights and the protection of socio-economic interests by the European Court of Human Rights* (diss. Leiden 2015).

Lodder e.a. 2014
A.R. Lodder e.a., *Big Data, Big Consequences*, Den Haag: WODC 2014.

Lodder & Schuilenburg 2016
A.R. Lodder & M.B. Schuilenburg, 'Politie-webcrawlers en Predictive policing', *Computerrecht* 2016/81, afl. 3, p. 150-153.

Loenen 2016
T. Loenen, 'Wijzigen of handhaven artikel 1 Grondwet: bij twijfel niet inhalen', 41 *Nederlands Tijdschrift voor Mensenrechten | NJCM-Bulletin* 2016, afl. 3, p. 319-326.

Loof 2013
J.P. Loof, 'Verbod van foltering en recht op bescherming van de lichamelijke en geestelijke integriteit', in: J.H. Gerards (red.), *Grondrechten. De nationale, Europese en internationale dimensie*, Nijmegen: Ars Aequi Libri 2013, p. 255-297.

Luan 2004
J. Luan, 'Data Mining Applications in Higher Education', *SPSS Executive Report* 2004, online via: http://www.spss.ch/upload/1122641492_Data%20mining%20applications%20in%20higher%20education.pdf.

Mačkić 2017
J. Mačkić, *Proving Discriminatory Violence at the Euopean Court of Human Rights* (diss. Leiden 2017).

Maple 2017
C. Maple, 'Security and privacy in the internet of things', *Journal of Cyber Policy*, afl. 2, p. 155-184.

Markou 2017
C. Markou, 'Why using AI to sentence criminals is a dangerous idea', *The conversation* 16 mei 2017, online via: https://theconversation.com/why-using-ai-to-sentence-criminals-is-a-dangerous-idea-77734.

Marr 2016
Bernard Marr, 'What Is The Difference Between Deep Learning, Machine Learning and AI?' *Forbes* 8 december 2016, online via: https://www.forbes.com/sites/bernardmarr/2016/12/08/what-is-the-difference-between-deep-learning-machine-learning-and-ai/#6e7e6e9526cf.

Mayer 2015
R. Mayer, 'Deep Learning Smarts Up Your Smart Phone', 8 december 2015, online via: https://www.amax.com/blog/?p=804.

Mayer-Schönberger & Cukier 2013
V. Mayer-Schönberger & K. Cukier, *Big Data: A revolution that will transform how we live, work and think*, New York: Houghton, Mifflin, Harcourt Publishing Company 2013.

McCarthy 2007
J. McCarty, 'What is artificial intelligence', 12 november 2007, via: http://jmc.stanford.edu/articles/whatisai/whatisai.pdf.

McKinsey 2011
McKinsey, *Big data: The next frontier for innovation, competition, and productivity*, mei 2011, online via: https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/big-data-the-next-frontier-for-innovation.

McKinsey 2015
McKinsey, *Unlocking the potential of the Internet of Things*, juni 2015, online via: https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/the-internet-of-things-the-value-of-digitizing-the-physical-world.

Meese 2017
J. Meese, 'C.7 Redelijke termijn', in: J.H. Gerards e.a. (red.), *Sdu Commentaar EVRM. Deel I – materiële rechten*, online via opmaat.sdu.nl, bijgewerkt tot en met 15 juni 2017.

Meuwese 2017
A.C.M. Meuwese, 'Grip op normstelling in het datatijdperk', in: W. den Ouden (red.), *Algemene regels in het bestuursrecht. VAR-preadviezen*, Den Haag: Boom juridische 2017.

Miller 2014
K. Miller, 'Total Surveillance, Big Data, and Predictive Crime Technology: Privacy's Perfect Storm', *Journal of Technology Law & Policy* 2014, p. 105-146.

Mirgaux 2015
S. Mirgaux, 'Artikel 13. Recht op een effectief rechtsmiddel', in J.H. Gerards e.a. (red.), *Sdu Commentaar EVRM. Deel I – materiële rechten*, online via opmaat.sdu.nl, bijgewerkt tot en met 15 juni 2015.

Mitchell 1997
T.M. Mitchell, *Machine Learning,* New York: McGraw-Hill Science 1997.

Miyakoshi & Kato 2011
Y. Miyakoshi & S. Kato. 'Facial Emotion Detection Considering Partial Occlusion Of Face Using Baysian Network', *Computers and Informatics* 2011, p. 96-101.

Moerel & Van der Wolk 2017
L. Moerel & A. van der Wolk, 'Big Data en het gegevensbeschermingsrecht', in: P.H. Blok (red.), *Big data en het recht: een overzicht van het juridisch kader voor big data-toepassingen in de private sector*, Den Haag: Sdu 2017, p. 37-72.

Mordini e.a. 2009
E. Mordini, D. Wright, K. Wadhwa, P. De Hert, E. Mantovani, J. Thestrup, G. van Steendam, A. D'Amico & I.Vater, 'Senior citizens and the ethics of e-inclusion', *Ethics and Information Technology* 2009, afl. 3, p. 203–220.

Morozov 2012
E. Morozov, *The Net Delusion: the Dark Side of Internet Freedom*, New York: Public Affairs 2012.

De Morree 2016
P.E. de Morree, *Rights and wrongs under the ECHR. The prohibition of abuse of rights in Article 17 of the European Convention on Human Rights* (diss. Utrecht 2016), Antwerpen: Intersentia 2016.

Muller 2017
C. Muller, *European Economic and Social Committee, Artificial intelligence, 'Opinion Section for the Single Market, Production and Consumption Artificial Intelligence – The Consequences of Artificial Intelligence on the (Digital) Single Market, Production, Consumption, Employment and Society*', 31 mei 2017, 7 (EESC Opinion), online via: http://www.eesc.europa.eu/en/our-work/opinions-information-reports/opinions/artificial-intelligence.

Nakad-Weststrate e.a. 2015
H.W.R. Nakad-Weststrate, H.J. van den Herik, A.W. Jongbloed, A-B. M. Salem, 'Digitally produced judgements in modern court proceedings', *International Journal for Digital Society* 2015, afl. 4, p. 1102-1112.

Nayyar, Puri & Le 2017
A. Nayyar, V. Puri & D-N. Le, 'Internet of Nano Things (IoNT): Next Evolutionary Step in Nanotechnology', *Nanoscience and Nanotechnology* 2017, afl. 1, p. 4-8.

Nehl 2014
H.P. Nehl, 'Article 48 (Administrative Law) – Presumption of Innocence and Rights of Defence', in: S. Peers e.a. (red.), *The EU Charter of Fundamental Rights. A Commentary*, Oxford/Portland: Hart 2014, p. 1278-1301.

Nehmelman 2002
R. Nehmelman, *Algemeen persoonlijkheidsrecht. Een rechtsvergelijkende studie naar het algemeen persoonlijkheidsrecht in Duitsland en Nederland* (diss. Utrecht 1992), Deventer: Kluwer 2002.

Nehmelman & Noorlander 2013
R. Nehmelman & C.W. Noorlander, *Horizontale werking van grondrechten, Over een leerstuk in ontwikkeling*, Deventer: Kluwer 2013.

Newman e.a. 2016
D. Newman, R. Fletcher, D.A.L. Levy & R.K. Nielsen, *Digital News Report 2016*, Oxford: Reuters Institute 2016.

New York Times 2017
'New Jersey Alters Its Bail System and Upends Legal Landscape', *New York Times* 6 februari 2017, online via: https://www.nytimes.com/2017/02/06/nyregion/new-jersey-bail-system.html.

Nieuwenhuis 2013a
A. Nieuwenhuis, 'Vrijheid van meningsuiting', in: J.H. Gerards e.a. (eindred.), *Grondrechten. De nationale, Europese en internationale dimensie*, Nijmegen: Ars Aequi Libri 2013, p. 71-104.

Nieuwenhuis 2013b
A. Nieuwenhuis, 'Vrijheid van gedachte, geweten, godsdienst en levensovertuiging', in: J.H. Gerards e.a. (eindred.), *Grondrechten. De nationale, Europese en internationale dimensie*, Nijmegen: Ars Aequi Libri 2013, p. 45-69.

Nieuwenhuis 2013c
A. Nieuwenhuis, 'Vrijheid van vereniging, vergadering en betoging', in: J.H. Gerards e.a. (red.), *Grondrechten. De nationale, Europese en internationale dimensie*, Nijmegen: Ars Aequi Libri 2013, p. 105-129.

Niklas, Sztanderska & Szymielewicz 2015
J. Niklas, K.S. Sztanderska & K. Szymielewicz, *Profiling the unemployed in Poland: Social and political implications of algorithmic decision making*, Warsaw: Creative Commons Attribution 4.0 International 2015.

Nilsson 2010
N.J. Nilsson, *The Quest for Artificial Intelligence. A history of ideas and achievements,* Cambridge: Cambridge University Press 2010.

Pandolfini 1997
B. Pandolfini, *Kasparov and Deep Blue: the Historic Chess Match between Man and Machine,* New York: Touchstone 1997.

Pariser 2011
E. Pariser, *The Filter Bubble: How the New Personalized Web Is Changing What We Read and How We Think*, Londen: Penguin Books 2011.

Pasquale 2015
F. Pasquale, *The Black Box Society. The Secret Algorithms That Control Money and Information*, Cambridge (MAS): Harvard University Press 2015.

Pasquale & Oren 2008
F. Pasquale & B. Oren, 'Federal Search Commission? Access, fairness and accountability in the law of search', *Cornell Law Review* 2008, afl. 6, p. 1167-1171.

Pech 2014
L. Pech, 'Article 47 – Right to an Effective Remedy. Article 47(2): Everyone is entitled to a fair and public hearing within a reasonable time *by an independent and impartial tribunal previously established by law*. Everyone shall have the possibility of being advised, defended and represented', in: S. Peers e.a. (red.), *The EU Charter of Fundamental Rights. A Commentary*, Oxford/Portland: Hart 2014, p. 1250-1258.

Peçi 2017
I. Peçi, 'C.4. Recht op een 'procedure op tegenspraak' ('right to an adversarial trial')', 'C.5 Motivering van rechterlijke uitspraken', 'C.6 Eerlijke en openbare behandeling', 'C.12 Voorbereiding verdediging' en 'C.16 Nemo tenetur: Het recht om te zwijgen en het recht tegen zelfincriminatie', in: J.H. Gerards e.a. (red.), *Sdu Commentaar EVRM. Deel I – materiële rechten*, online via opmaat.sdu.nl, bijgewerkt tot en met 15 juni 2017.

Perry 2013
W.L. Perry 2013, *Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations*, Rand Corporation. Safety and Justice Program 2013, online via; https://www.rand.org/content/dam/rand/pubs/research_reports/RR200/RR233/RAND_RR233.pdf (laatst geraadpleegd 21 december 2017).

Perry & Roda 2017
S. Perry & C. Roda, *Human Rights and Digital Technology. Digital Tightrope*, Londen: Palgrave Macmillan 2017.

Peppet 2014
S.R. Peppet, 'Regulating the Internet of Things: First steps towards managing discrimination, Privacy, Security and Consent', *Texas Law Review* 2014, p. 85-176.

Poudel 2016
S. Poudel, 'Internet of Things: underlying technologies, interoperability, and threats to privacy and security', *Berkeley Technology Law Journal* 2016, afl. 2, p. 997-1022.

Van der Pot/Donner 2006
C.W. van der Pot, bew. door D.J. Elzinga, R. de Lange & H.G. Hoogers, *Handboek van het Nederlandse staatsrecht*, Deventer: Kluwer 2006.

Prakken 2018
H. Prakken, 'Komt de robotrechter er aan?', *Nederlands Juristenblad* 2018, afl. 4, p. 269-274.

Prins 2017
M.A. Prins, 'Een koelkast als getuige. Over de (toekomstige) rol van de Internet of Things in de opsporing', *Tijdschrift Praktijkwijzer Strafrecht* 2017, afl. 22, p. 112-117.

Prins & Van der Roest 2018
J.E.J. Prins & Jurgen van der Roest, 'AI en de rechtspraak: Meer dan alleen de 'robotrechter'', *Nederlands Juristenblad,* afl. 4, p. 260-268.

Reiertsen 2017
M. Reiertsen, *The European Convention on Human Rights Article 13. Past, Present and Future* (diss. University of Oslo 2017).

Richards 2008
N.M. Richards, 'Intellectual Privacy', *Texas Law Review* 2008, p. 388-455.

Richards & King 2013
N.M. Richards & J.H. King, 'Three Paradoxes of Big Data', *Stanford Law Review Online* 2013, p. 41-46.

Roorda 2016
B. Roorda, *Het recht om te demonstreren. Een vergelijkende studie naar de betogingsvrijheid in Nederland, Duitsland en Engeland vanuit internationaalrechtelijk perspectief* (diss. Groningen 2016), Den Haag: Boom juridisch 2016.

Rosenblat, Kneese & Boyd 2014
A. Rosenblat, T. Kneese & D. Boyd, 'Networked Employment Discrimination', *Data & Society Research Institute Open Society Foundations' Future of Work Commissioned Research Papers,* online via SSRN: https://ssrn.com/abstract=2543507.

Rouse 2017
M. Rouse, 'Definition. Machine Leaning', juni 2017, online via: http://whatis.techtarget.com/definition/machine-learning.

Rouvroy 2015
A. Rouvroy, '*Of Data and Men': Fundamental Rights and Liberties in a World of Big Data*', Straatsburg: Raad van Europa 2016.

Russel & Norvig 2010
S.J. Russell & P. Norvig, *Artifical Intelligence. A Modern Approach*, New York: Pearson Education, Inc. 2010.

Samuel 1959
A.L. Samuel, 'Some Studies in Machine Learning Using the Game of Checkers'. *IBM Journal of Research and Development* 1959, p. 535-554.

Sanderink 2015
D.G.J. Sanderink, *Het EVRM en het materiële omgevingsrecht* (diss. Nijmegen), Kluwer: Deventer 2015.

Van Sasse van Ysselt 2017
P.B.C.D.F. van Sasse van Ysselt, 'Realisering van het recht op onaantastbaarheid van het lichaam door middel van wetgeving', *RegelMaat* 2017, afl. 6, p. 403-418.

Van Sasse van Ysselt 2017b
P.B.C.D.F. van Sasse van Ysselt, *Realisering van grondrechten. De rechtsplicht van de overheid tot de verwerkelijking van grondrechten bij botsende rationaliteiten en belangen in een rechtspolitieke context* (diss. VU Amsterdam 2017).

Sayers 2014
D. Sayers, 'Article 47 – Right to an Effective Remedy. Article 47(2): Everyone is entitled to *a fair and public hearing within a reasonable time* by an independent and impartial tribunal previously established by law. Everyone shall have the possibility of being advised, defended and represented', in: S. Peers e.a. (red.), *The EU Charter of Fundamental Rights. A Commentary*, Oxford/Portland: Hart 2014, p. 1258-1269.

Sayers 2014b
D. Sayers, 'Article 48 (Criminal Law) – Presumption of Innocence and Rights of Defence', in: S. Peers e.a. (red.), *The EU Charter of Fundamental Rights. A Commentary*, Oxford/Portland: Hart 2014, p. 1304-1349.

Scherer 2016
M.U. Scherer, 'Regulating Artificial Intelligence Systems: Risks, Challenges, Competencies, and Strategies', *Harvard Journal of Law & Technology* 2016, afl. 2, p. 353-400.

Schermer 2011
B.W. Schermer, 'The limits of privacy in automated profiling and data mining', *Computer law & security review* 2011, p. 45-52.

Schermer & Wagemans 2009
B.W. Schermer & T. Wagemans, *Onze digitale schaduw. Een verkennend onderzoek naar het aantal databases waarin de gemiddelde Nederlander geregistreerd staat*, 23 januari 2009, online via: https://autoriteitpersoonsgegevens.nl/sites/default/files/downloads/rapporten/rap_2009_onze_digitale_schaduw.pdf.

Schiek 2007
D. Schiek, 'Indirect Discrimination', in: Bell, M., Schiek, D. & Waddington, L. (red.), *Cases, Materials and Text on National, Supranational and International Non-Discrimination Law*, Oxford: Hart Legal Publishers 2007, p. 323-475.

Schiek & Chege 2009
D. Schiek & V. Chege (red.), *European Union Non-Discrimination Law. Comparative Perspectives on Multidimensional Equality Law*, Abingdon: Routledge 2009.

Schuurmans 2005
Y.E. Schuurmans, *Bewijslastverdeling in het bestuursrecht. Zorgvuldigheid en bewijsvoering bij beschikkingen* (diss. VU Amsterdam 2005), Deventer: Kluwer 2005.

Schuyt 2008
K. Schuyt, 'Wetten veranderen, het geweten blijft', in: J.P. Loof (red.), *Juridische ruimte voor gewetensbezwaren?*, Leiden: Stichting NJCM Boekerij 2008, p. 1-17.

Sethi & Sarangi 2017
P. Sethi & S.R. Sarangi, 'Internet of Things: Architectures, Protocols, and Applications', *Journal of Electrical and Computer Engineering* 26 januari 2017, article ID 9324035, online via: https://www.hindawi.com/journals/jece/2017/9324035/.

Sharkey 2014
A. Sharkey, 'Robots and human dignity: A consideration of the effects of robot care on the dignity of older people', *Ethics and Information Technology*, afl. 1, p. 63-75.

Sharkey & Sharkey 2010
A. Sharkey & N. Sharkey, 'Granny and the robots: Ethical issues in robot care for the elderly'. *Ethics and Information Technology* 2010, afl. 1, p. 27–40.

Sharma, Mittal & Garg 2016
Y. Sharma, E. Mittal & M. Garg, 'Political Opinion Mining from Twitter', *International Journal of Information Systems in the Service Sector* 2016, afl. 4, p. 47-56.

Shelton 2014
D. Shelton, 'Article 47 – Right to an Effective Remedy. Sources of Article 47 Rights', in: S. Peers e.a. (red.), *The EU Charter of Fundamental Rights. A Commentary*, Oxford/Portland: Hart 2014, p. 1200-1210.

Singhal 2015
A. Singhal, 'A Flawed Elections Conspiracy Theory', 26 augustus 2015, via: https://www.politico.com/magazine/story/2015/08/google-2016-election-121766.

Van der Sloot 2016
B. van der Sloot, 'Is the Human Rights Framework Still Fit for the Big Data Era? A Discussion of the ECtHR's Case Law on Privacy Violations Arising from Surveillance Activities', in: S. Gutwirth, R. Leenes & P. de Hert (red.), *Data Protection on the Move. Current Developments in ICT and Privacy/Data Protection*, Springer 2016, p. 423-426.

Smet 2010
S. Smet, 'Freedom of Expression and the Right to Reputation: Human Rights in Conflict', 26 *American University International Law Review* 2010, afl. 1, p. 183-236.

Smet 2015
S. Smet, 'Artikel 8. Naamrecht, eer en goede naam, reputatie', in: J.H. Gerards e.a. (red.), *Sdu Commentaar EVRM. Deel I – materiële rechten*, online via opmaat.sdu.nl, bijgewerkt tot en met 15 juni 2015.

Solove 2006
D.J. Solove, 'A Taxonomy of Privacy', *University of Pennsylvania Law Review* 2006, p. 477-564.

Special Rapporteur on Freedom of Opinion and Expression 2016
Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, *2016 Report of the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye, to the 32nd session of the Human Rights Councilon Freedom of expression, states and the private sector in the digital age* (A/HRC/32/38).

Special Rapporteur on Freedom of Opinion and Expression 2017
Special Rapporteur on the promotion and protection of the right to freedom of opinion and expres-sion, *2017 Report of the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye, to the 35th session of the Human Rights Council on the Role of Digital Access Providers* (A/HRC/35/22).

Staatscommissie Grondwet 2010
Staatscommissie Grondwet, *Rapport Staatscommissie Grondwet*, Den Haag, november 2010, bijlage bij *Kamerstukken II* 2010/11, 31570, nr. 17.

Staatscommissie parlementair stelsel 2017
Staatscommissie parlementair stelsel, *Probleemverkenning staatscommissie parlementair stelsel*, Den Haag 2017, bijlage bij *Kamerstukken II* 2017/18, 34430, nr. 5.

Statrix 2015
Statrix, *Internet of Things in the Netherlands. Applications, trends and potential impact on radio spectrum,* September 2015, online via: https://www.rijksoverheid.nl/documenten/rapporten/2015/10/08/internet-of-things-in-the-netherlands.

Steenbruggen & Zwenne 2017
W.A.M. Steenbruggen & G.J. Zwenne, 'Privacyrisico's en -waarborgen bij het gebruik van big data tegen zorgfraude: een verkenning', in: *Big data in de zorg. Preadvies 2017*, Den Haag: Sdu 2017.

Steppe 2017
R. Steppe, 'Online price discrimination and personal data: A General Data Protection Regulation perspective', *Computer law & security review* 2017, afl. 6, p. 768-785.

Sunstein 2001
C.R. Sunstein, *Republic.com 2.0*, Princeton: Princeton University Press 2001.

Squires 2003
G. Squires, 'Racial profiling, insurance style: insurance redlining and the uneven development of metropolitan areas', *Journal of Urban Affairs* 2003, afl. 4, p. 391-410.

Taylor 2013
C. Taylor,'Big Data's slippery issue of causation vs. correlation', *Wired* 15 juli 2013, online via: http://insights.wired.com/profiles/blogs/big-data-s-slippery-issue-of-causation-versus-correlation.

Terry 2016
N.P. Terry, 'Will the Internet of Things Transform Healthcare', *Vanderbilt Journal of Entertainment & Technology Law* 2016, afl. 2, p. 327-352.

Timmer 2011
A. Timmer, 'Toward an Anti-Stereotyping Approach for the European Court of Human Rights', 11 *Human Rights Law Review* 2011, afl. 4, p. 707-738.

Timmer 2013
A. Timmer, 'A Quiet Revolution: Vulnerability in the European Court of Human Rights', in: M. Fineman & A. Grear (red.), *Vulnerability: Reflections on a New Ethical Foundation for Law and Politics*, Farham: Ashgate 2013, p. 147-170.

Timmer e.a. 2015
T. Timmer, I. Elias, L. Kool & R. van Est, *Berekende risico's. Verzekeren in de datagedreven samenleving*, Den Haag: Rathenau Instituut 2015.

Tobler 2005
Ch. Tobler, *Indirect Discrimination. A Case Study into the Development of the Legal Concept of Indirect Discrimination under EC Law*, Antwerpen: Intersentia 2005.

Tufekci 2018
Z. Tufekci, 'It's The (Democracy-Poisoning) Golden Age of Free Speech', *Wired* 16 January 2018, via: https://www.wired.com/story/free-speech-issue-tech-turmoil-new-censorship/.

Turing 1950
A.M. Turing, 'Computing Machinery and Intelligence', *Mind* 1950, p. 433-460.

Tushnet 2008
R. Tushnet, 'Power without responsibility: intermediaries and the First Amendment', *George Washington Law Review* 2008, afl. 4, p. 1015-1016.

UK Information Commissioner
UK Information Commissioner, *Big data, artificial intelligence, machine learning and data protection*, 4 september 2017, online via: https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf.

UN Special Rapporteur on extrajudicial, summary or arbitrary executions 2013
UN Special Rapporteur on extrajudicial, summary or arbitrary executions, *2013 Report of the UN Special Rapporteur on extrajudicial, summary or arbitrary exe-cutions, Christof Heyns, to the 25th session of the Human Rights Council* (A/HRC/26/36).

Vedder 1999
A. Vedder, 'KDD: The challenge to individualism', *Ethics and Information Technology* 1999, afl. 1, p. 275-281.

Vedder & Naudts 2017
A. Vedder & L. Naudts, 'Accountability for the use of algorithms in a big data environment', *International Review of Law, Computers & Technology* 2017, afl. 2, p. 206-224.

Verhey 1992
L.F.M. Verhey, *Horizontale werking van grondrechten, in het bijzonder van het recht op privacy* (diss. Utrecht 1992), Zwolle: W.E.J. Tjeenk Willink 1992.

Verhey 2009
L.F.M. Verhey, 'Horizontale werking van grondrechten: de stille Straatsburgse revolutie', in: T. Barkhuysen, M.L. van Emmerik & J.P. Loof (red.), *Geschakeld recht, Verdere studies over Europese grondrechten ter gelegenheid van de 70ste verjaardag van prof. mr. E.A. Alkema*, Deventer: Kluwer 2009.

Vermeulen 1989
B.P. Vermeulen, *De vrijheid van geweten een fundamenteel rechtsprobleem* (diss. Rotterdam), Arnhem: Gouda Quint 1989.

Vermeulen 2006
B.P. Vermeulen, 'Kerkgenootschap en geestelijk ambt', in: M.L.M. Hertogh & P.J.J. Zoontjens (red.), *Gelijke behandeling: principes en praktijken. Evaluatieonderzoek Algemene wet gelijke behandeling*, Nijmegen: WLP 2006, p. 219-249.

Vermeulen 2009
B.P. Vermeulen, 'Gewetensvrijheid en godsdienstvrijheid in de neutrale staat', in: F.T. Oldenhuis (red.), *Een neutrale staat: kreet of credo?*, Heerenveen: Protestantse Pers 2009, p. 74-103.

Vermeulen & Van Roosmalen 2018
B.P. Vermeulen & M. van Roosmalen, 'Chapter 13. Freedom of thought, conscience and religion', in: P. van Dijk, F. van Hoof e.a. (red.), *Theory and Practice of the European Convention on Human Rights*, Antwerpen: Intersentia 2018, p. 735-763.

Vetter 1995
R.J. Vetter, 'Internet Kiosk-Computer-Controlled Devices Reach the Internet.', *Computer* 1995, afl. 12, p. 66–67.

Vīķe-Freiberga e.a. 2013
V. Vīķe-Freiberga, H. Däubler-Gmelin, B. Hammersley & L.M.P. Pessoa Maduro, *A free and pluralistic media to sustain European democracy* 2013, https://ec.europa.eu/digital-single-market/sites/digital-agenda/files/HLG%20Final%20Report.pdf.

Villaronga, Kieseberg & Li 2017
E.F. Villaronga, P. Kieseberg & T. Li, 'Humans forget, machines remember: Artificial Intelligence and the Right to Be Forgotten', *Computer Law and Security Review* 2017, p. 1-10.

De Vocht 2017
D. de Vocht, 'C.3 Gegrondheid vervolging', in: J.H. Gerards e.a. (red.), *Sdu Commentaar EVRM. Deel I – materiële rechten*, online via opmaat.sdu.nl, bijgewerkt tot en met 15 juni 2017.

De Vries 2013
K. de Vries, 'Het recht op privéleven en aanverwante rechten', in: J.H. Gerards e.a. (red.), *Grondrechten. De nationale, Europese en internationale dimensie*, Nijmegen: Ars Aequi Libri 2013.

De Vries 2018
K. de Vries, 'Chapter 12. Right to respect for private and family life', in: P. van Dijk, F. van Hoof e.a. (red.), *Theory and Practice of the European Convention on Human Rights*, Antwerpen: Intersentia 2018, p. 667-733.

Wagner 2017
B. Wagner, *Council of Europe, Committee of Experts on Internet Intermediaries (MSI-NET), Draft report on the human rights dimensions of algorithms - second draft (20 february 2017*), online via: https://rm.coe.int/16806fe644.

Warren & Brandeis 1890
S.D. Warren & L. Brandeis, 'The Right to Privacy', *Harvard Law Review* 1890, p. 193-220.

Weber & Studer 2016
R.H. Weber & E. Studer, 'Cybersecurity in the internet of things: legal aspects', *Computer Law and Security Review* 2016, p. 715–728.

White 2015
T. White, *Hadoop. The definitive guide*, O'Reilly Media 2015.

White House 2014a
White House, *Big Data. Seizing opportunities, preserving values*, Washington DC: Executive Office of the President mei 2014, online via:https://obamawhitehouse.archives.gov/sites/default/files/docs/ big_data_privacy_report_may_1_2014.pdf.

White House 2014b
White House, *Big Data and privacy: a technological perspective*, Washington DC: Executive Office of the President and the President's Council of Advisors on Science and Technology mei 2014, online via: https://bigdatawg.nist.gov/pdf/pcast_big_data_and_privacy_-_may_2014.pdf.

White House 2016
White House, *Big Data: A Report on Algorithmic Systems, Opportunity, and Civil Rights*, Washington DC: Executive Office of the president mei 2016, online via: https://obamaw-

hitehouse.archives.gov/sites/default/files/microsites/ostp/2016_0504_data_discrimination.pdf.

Wiarda 1987
G.J. Wiarda, *Advies betreffende de verenigbaarheid van een eventueel in te voeren identificatieplicht met internationale en nationale bepalingen inzake grondrechten*, 2 juni 1987, *Kamerstukken II* 1986/87, 19 991, nr. 1.

Widdershoven 2016
R.J.G.M. Widdershoven, 'De redelijke termijn tussen Nederland, Luxemburg en Straatsburg', in: R. Ortlep e.a., *De rechter onder vuur*, Oisterwijk: WLP 2016, p. 63-76.

Willems 2014
D. Willems, 'Predictive Policing: wens of werkelijkheid?', *Tijdschrift voor de Politie* 2014, afl. 4/5, p. 39-42.

Witteman 2017
K. Witteman, 'C.2. Civil Rights and Obligations', in: J.H. Gerards e.a. (red.), *Sdu Commentaar EVRM. Deel I – materiële rechten*, online via opmaat.sdu.nl, bijgewerkt tot en met 15 juni 2017.

Woolley & Howard 2016
S.C. Woolley & P.N. Howard, 'Political Communication, Computational Propaganda, and Autonomous Agents', 10 *International Journal of Communication* 2016, p. 4882–4890.

WRR 2016
Wetenschappelijke Raad voor het Regeringsbeleid, *Big Data in een vrije en veilige samenleving* (rapport nr. 95), Den Haag 2016, online via: https://www.wrr.nl/onderwerpen/big-data-privacy-en-veiligheid/documenten/rapporten/2016/04/28/big-data-in-een-vrije-en-veilige-samenleving.

Zarsky 2003
T.Z. Zarsky, 'Mine your own business: making the case for the implications of the data mining of personal information in the forum of public opinion', *Yale Journal of Law and Technology* 2003, afl. 5, p. 1-56.

Ziegeldorf, Morchon & Wehrle 2013
J.H. Ziegeldorf, O. Garcia Morchon & K. Wehrle, 'Privacy in the Internet of Things: threats and challenges', *Security and Communication Networks* 2014, afl. 7, p. 2728–2742.

Žliobaitė & Custers
I. Žliobaitė & B.H.M. Custers, 'Using sensitive personal data may be necessary for avoiding discrimination in data-driven decision models', *Artificial Intelligence and Law* 2016, afl. 2, p. 183-201.

Van Zoonen 2016
L. van Zoonen, 'Privacy concerns in smart cities', *Government Information Quarterly* 2016, afl. 3, p. 475-476.

Zuiderveen Borgesius 2014
F.J. Zuiderveen Borgesius, *Improving privacy protection in the area of behavioural targeting* (diss. Amsterdm UvA), Alphen aan den Rijn: Kluwer Law International 2014.

Zuiderveen Borgesius 2017
F.J. Zuiderveen Borgesius & J. Poort, 'Online Price Discrimination and EU Data Privacy Law', *Journal of Consumer Policy* 2017, afl. 3, p. 347-366.

Zuiderveen Borgesius e.a. 2016
F.J. Zuiderveen Borgesius, D. Trilling, J. Möller, S. Eskens, B. Bodó, C.H. de Vreese & N. Helberge, 'Algoritmische verzuiling en filter bubbles: een bedreiging voor de democratie?', *Computerrecht* 2016/173, afl. 5, p. 255-262.

Zuiderveen Borgesius e.a. 2018
F.J. Zuiderveen Borgesius, J. Möller, S. Kruikemeier, R. Fathaigh, K. Irion, T. Dobber, B. Bodo & C. Vreese, 'Online Political Microtargeting: Promises and Threats for Democracy', *Utrecht Law Review* 2018, afl. 1, p. 82-96.

Jurisprudentie

Hof van Justitie van de Europese Unie

HvJ 1 maart 2011, zaak C-236/09, ECLI:EU:C:2011:100 (*Test-Achats*), *EHRC* 2011/64 m.nt. Y. Thiery, *NJ* 2011/120 m.nt. M.R. Mok.

HvJ 17 juli 2008, zaak C-303/06, ECLI:EU:C:2008:415 (*Coleman*), *EHRC* 2008/108 m.nt. A.C. Hendriks, *NJ* 2008/501 m.nt. M.R. Mok, TRA 2008 m.nt. A. Veldman.

HvJ EU 22 december 2010, zaak C-208/09, ECLI:EU:C:2010:806 (*Sayn-Wittgenstein*), *NJ* 2011/119 m.nt. M.R. Mok.

HvJ EU 12 mei 2011, zaak C-391/09, ECLI:EU:C:2011:291 (*Runevič-Vardyn en Wardyn*), *NJ* 2011/421 m.nt. M.R. Mok.

HvJ EU 18 oktober 2011, zaak C-34/10, ECLI:EU:C:2011:669 (*Brüstle*), *EHRC* 2012/54 m.nt. F.M. Fleurke, *NTM-NJCM-Bull.* 2012, p. 242 m.nt. B. van Beers.

HvJ EU 5 september 2012, gev. zaken C-71/11 en C-99/11, ECLI:EU:C:2012:518 (*Y en Z*), *EHRC* 2003/1 m.nt. B. Aarrass & K.M. de Vries, *JV* 2012/403 m.nt. H. Battjes.

HvJ 6 november 2012, zaak C-199/11, ECLI:EU:C:2012:684 (*Otis*), *EHRC* 2013/3 m.nt. C. Mak, *NJ* 2013/168 m.nt. M.R. Mok.

HvJ EU 4 juni 2013, zaak C-300/11, ECLI:EU:C:2013:363, *EHRC* 2013/160 m.nt. A. Woltjer, *AB* 2013/374 m.nt. M. Reneman.

Gerecht 13 september 2013, zaak T-383/11, ECLI:EU:T:2013:431 (*Makhlouf*), *EHRC* 2013/231.

HvJ EU 18 juli 2013, gev. zaken C-584/10 P, C-593/10 P en C-595/10 P, ECLI:EU:C:2013:518 (*Kadi*), *EHRC* 2013/229 m.nt. S.J. Hollenberg.

HvJ EU 17 oktober 2013, zaak C-291/12, ECLI:EU:C:2013:670 (*Schwarz*), *EHRC* 2014/6 m.nt. D. Groenenberg, *AB* 2014/129 m.nt. A.M. Klingenberg.

HvJ 8 april 2014, gev. zaken C-293/12 en C-594/12, ECLI:EU:C:2014:238 (*Digital Rights Ireland*), *EHRC* 2014/140 m.nt. M.E. Koning, *NJ* 2016/446 m.nt. E.J. Dommering.

HvJ EU 13 mei 2014, C-131/12, ECLI:EU:C:2014:317 (*Google Spain*), *EHRC* 2014/186, m.nt. J.V.J. van Hoboken, *NJ* 2014/385 m.nt. M.R. Mok.

HvJ EU 18 juni 2015, zaak C-583/13 P, ECLI:EU:C:2015:404 (*Deutsche Bahn*).

HvJ 5 april 2016, gev. zaken C-404/15 en C-659/15 PPU, ECLI:EU:C:2016:198 (*Aranyosi en Căldăraru*), *EHRC* 2016/157 m.nt. H. van der Wilt.

HvJ EU 2 juni 2016, zaak C-438/14, ECLI:EU:C:2016:401 (*Bogendorff von Wolffersdorff*), *EHRC* 2016/202 m.nt. D.A.J.G. de Groot.

HvJ EU 13 september 2016, zaak C-165/14, ECLI:EU:C:2016:675 (*Rendón Marín*), *JV* 2016/201.

HvJ EU 14 maart 2017, zaak C-157/15, ECLI:EU:C:2017:203 (*Achbita*), *EHRC* 2017/96 m.nt. J.H. Gerards, *AB* 2017/162 m.nt. M.L.P. Loenen, *JAR* 2017/96 m.nt. E. Cremers-Hartman, *TRA* 2017/66 m.nt. N. Gundt.

HvJ EU 14 maart 2017, zaak C-188/15, ECLI:EU:C:2017:204 (*Bougnaoui*), *EHRC* 2017/97 m.nt. J.H. Gerards onder *EHRC* 2017/96, *AB* 2017/163 m.nt. M.L.P. Loenen, *JAR* 2017/97 m.nt. E. Cremers-Hartman.

Gerecht EU 15 juni 2017, zaak T-262/15, ECLI:EU:T:2017:392 *(Kiselev*), *EHRC* 2017/154 m.nt. P.E. De Morree.

Hof van Justitie van de Europese Gemeenschappen

HvJ EG 21 september 1989, gev. zaken 46/87 en 227/88 (*Hoechst AG*).

HvJ EG 17 oktober 1989, zaak 85/87 (*Dow Benelux NV*).

HvJ EG 22 oktober 2002, zaak C-94/00 (*Roquette Frères SA*).

HvJ EG 2 oktober 2003, zaak C-148/02 (*Garcia Avello*).

Europees Hof voor de Rechten van de Mens

EHRM 8 juni 1976, nrs. 5100/71 e.a., ECLI:CE:ECHR:1976:1123JUD000510071 (*Engel e.a. t. Nederland*), *NJ* 1978/223, *AB* 1978/223 m.nt. J. in 't Veld.

EHRM 7 december 1976, nr. 5493/72, ECLI:CE:ECHR:1976:1207JUD000549372 (*Handyside t. het Verenigd Koninkrijk*).

EHRM 6 september 1978, nr. 5029/71, ECLI:CE:ECHR:1978:0906JUD000502971 (*Klass e.a. t. Duitsland*), *NJ* 1979/327 m.nt. E.A. Alkema.

EHRM 26 april 1979, nr. 6538/74, ECLI:CE:ECHR:1979:0426JUD000653874 (*Sunday Times t. het Verenigd Koninkrijk*).

EHRM 23 juni 1981, nrs. 6878/75 en 7238/75, ECLI:CE:ECHR:1982:1018JUD000687875 (*Le Compte, Van Leuven en De Meyere t. België*).

EHRM 22 oktober 1981, nr. 7525/76, ECLI:CE:ECHR:1981:1022JUD000752576 (*Dudgeon t. het Verenigd Koninkrijk*).

EHRM 2 augustus 1984, nr. 8691/79, ECLI:CE:ECHR:1984:0802JUD000869179 (*Malone t. het Verenigd Koninkrijk*), *NJ* 1988/534 m.nt. P. van Dijk.

EHRM 26 maart 1985, nr. 8978/80, ECLI:CE:ECHR:1985:0326JUD000897880 (*X. en Y. t. Nederland*), *NJ* 1985/525 m.nt. E.A. Alkema, *NJCM-Bull.* 1985, p. 410 m.nt. J.G.C. Schokkenbroek.

EHRM 2 maart 1987, nr. 9267/81, ECLI:CE:ECHR:1987:0302JUD000926781 (*Mathieu-Mohin en Clerfayt t. België*).

EHRM 21 juni 1988, nr. 10126/82, ECLI:CE:ECHR:1988:0621JUD001012682 (*Plattform 'Ärzte für das Leben' t. Oostenrijk*).

EHRM 7 juli 1989, nr. 10454/83 (*Gaskin t. Verenigd Koninkrijk*), ECLI:NL:XX:1989:AB9903, *NJ* 1991/659, m.nt. E.J. Dommering.

EHRM 24 april 1990, nr. 11801/85, ECLI:CE:ECHR:1990:0424JUD001180185 (*Kruslin t. Frankrijk*), *NJ* 1991/523 m.nt. E.J. Dommering.

EHRM 16 december 1992, nr. 13710/88, ECLI:CE:ECHR:1992:1216JUD001371088 (*Niemietz t. Duitsland*), *NJ* 1993/400, m.nt. E.J. Dommering.

EHRM 30 juni 1993 (*Sigurdur A. Sigurjónsson t. IJsland*), nr. 16130/90, ECLI:CE:ECHR:1993:0630JUD001613090.

EHRM 26 september 1995, nr. 17851/91, ECLI:CE:ECHR:1995:0926JUD001785191 (*Vogt t. Duitsland*).

EHRM (GK) 30 januari 1998, nr. 19392/92, ECLI:CE:ECHR:1998:0130JUD001939292 (*United Communist Party of Turkey e.a. t. Turkije*).

EHRM (GK) 18 februari 1999, nr. 24833/94, ECLI:CE:ECHR:1999:0218JUD002483394 (*Matthews t. het Verenigd Koninkrijk*), *JB* 1999/64, *AB* 1999/181 m.nt. I. Sewandono, *NJ* 1999/515 m.nt. E.A. Alkema.

EHRM (GK) 29 april 1999, nr. 25088/94 e.a., ECLI:CE:ECHR:1999:0429JUD002508894 (*Chassagnou t. Frankrijk*), *JB* 1999/186 m.nt. Heringa.

EHRM (GK) 27 september 1999, nrs. 33985/96 en 33986/96, ECLI:CE:ECHR:1999:0927JUD0033985-96 (*Smith en Grady t. het Verenigd Koninkrijk*).

EHRM 14 december 1999, nr. 38178/97, ECLI:CE:ECHR:1999:1214JUD003817897 (*Serif t. Griekenland*), *EHRC* 2000/14 m.nt. A.W. Heringa, *AB* 2000/73 m.nt. I. Sewandono.

EHRM (GK) 27 juni 2000, nr. 27417/95, ECLI:CE:ECHR:2000:0627JUD002741795 (*Cha'are Shalom ve Tsedek t. Frankrijk*), *EHRC* 2000/66 m.nt. J.H. Gerards, *AB* 2001/116 m.nt. B.P. Vermeulen, *NJCM-Bull.* 2001, p. 328 m.nt. C.D. de Jong.

EHRM 6 februari 2001, nr. 44599/98, ECLI:CE:ECHR:2001:0206JUD004459998 (*Bensaid t. het Verenigd Koninkrijk*), *NJ* 2001/549, *JV* 2001/103 m.nt. Wouters.

EHRM 7 juni 2001 (GK), nr. 39594/98, ECLI:CE:ECHR:2001:0607JUD003959498 (*Kress t. Frankrijk*), EHRC 2001/51 m.nt. A.W. Heringa.

EHRM 7 juni 2001 (ontv.), nr. 56618/00, ECLI:CE:ECHR:2001:0607DEC005661800 (*Federacion Nacionalista Canaria t. Spanje*).

EHRM 25 september 2001, nr. 44787/98, ECLI:CE:ECHR:2001:0925JUD004478798 (*P.G. en J.H. t. het Verenigd Koninkrijk*).

EHRM 7 februari 2002, nr. 53176/99, ECLI:CE:ECHR:2002:0207JUD005317699 (*Mikulić t. Kroatië*), *EHRC* 2002/25 m.nt. H.L. Janssen.

EHRM 9 april 2002, nr. 46726/99, ECLI:CE:ECHR:2002:0409JUD004672699 (*Podkolzina t. Letland*), *EHRC* 2002/41 m.nt. A.W. Heringa.

EHRM 29 april 2002, nr. 2346/02, ECLI:NL:XX:2002:AP0678 (*Pretty t. het Verenigd Koninkrijk*), *EHRC* 2002/47, m.nt. Gerards & Janssen, *NJ* 2004/543 m.nt. E.A. Alkema, *NJCM-Bull.* 2002, p. 910 m.nt. B.E.P. Myjer.

EHRM 2 juli 2002 (ontv.), nr. 53180/99, ECLI:CE:ECHR:2002:0702DEC005318099 (*Gorizdra t. Moldavië*).

EHRM (GK) 11 juli 2002, nr. 28957/95, ECLI:CE:ECHR:2002:0711JUD002895795 (*Christine Goodwin t. het Verenigd Koninkrijk*), *EHRC* 2002/74 m.nt. H.L. Janssen & J. van der Velde.

EHRM 28 januari 2003, nr. 44647/98, ECLI:CE:ECHR:2003:0128JUD004464798 (*Peck t. het Verenigd Koninkrijk*), *EHRC* 2003/24.

EHRM (GK) 13 februari 2003, nrs. 1340/98 e.a., ECLI:CE:ECHR:2003:0213JUD004134098 (*Refah Partisi e.a. t. Turkije*), *EHRC* 2003/28 m.nt. H.L. Janssen, *NJ* 2005/73 m.nt. E.A. Alkema, *AB* 2002/179 m.nt. M.J. Kanne.

EHRM (GK) 6 maart 2003, nr. 58278/00, ECLI:CE:ECHR:2006:0316JUD005827800 (*Ždanoka t. Letland*), *EHRC* 2004/76.

EHRM 12 juni 2003, nr. 35968/97, ECLI:CE:ECHR:2003:0612JUD003596897 (*Van Kück t. Duitsland*), *EHRC* 2003/61 m.nt. J.H. Gerards, *AB* 2003/437 m.nt. B. van Beers.

EHRM (GK) 8 juli 2003, nr. 36022/97, ECLI:CE:ECHR:2003:0708JUD003602297 (*Hatton t. het Verenigd Koninkrijk*), *EHRC* 2003/71 m.nt. H.L. Janssen, *AB* 2003/445 m.nt. A. Woltjer, *NJ* 2004/207 m.nt. E.J. Dommering.

EHRM 8 juli 2003 (ontv.), nr. 27677/02, ECLI:CE:ECHR:2003:0708DEC002767702 (*Sentges t. Nederland*), *EHRC* 2003/75 m.nt. E. Brems, *NJCM-Bull.* 2004, p. 54 m.nt. A.C. Hendriks.

EHRM 17 juli 2003, nr. 63737/00 (*Perry/Verenigd Koninkrijk*), *NJ* 2006/40 m.nt. E.J. Dommering, *EHRC* 2003/79.

EHRM 22 juli 2003, nr. 24209/94, ECLI:CE:ECHR:2014:1106JUD001292713 (*Y.F. t. Turkije*), *EHRC* 2003/80 m.nt. K. Henrard.

EHRM (GK) 9 oktober 2003, nr. 48321/99, ECLI:CE:ECHR:2003:1009JUD004832199 (*Slivenko t. Letland*), *EHRC* 2003/91 m.nt. H.L. Janssen.

EHRM (GK) 17 februari 2004, nr. 44158/98, ECLI:CE:ECHR:2004:0217JUD004415898 (*Gorzelik e.a. t. Polen*), *EHRC* 2004/32 m.nt. H.L. Janssen, *NJ* 2005/420 m.nt. E.A. Alkema, *AB* 2002/180 m.nt. M.J. Kanne.

EHRM 1 juli 2004, nr. 69498/01, ECLI:CE:ECHR:2004:0713JUD006949801 (*Pla en Puncernau t. Andorra*), *EHRC* 2004/87 m.nt. E. Brems, *NJ* 2005/508 m.nt. J. de Boer.

EHRM 27 juli 2004, nr. 55480/00, ECLI:CE:ECHR:2004:0727JUD005548000 (*Sidabras en Džiautas t. Litouwen*), *EHRC* 2004/90, m.nt. Gerards.

EHRM 16 november 2004, nr. 4143/02, ECLI:CE:ECHR:2004:1116JUD000414302 (*Moreno Gómez t. Spanje*), *EHRC* 2005/12 m.nt. H.L. Janssen, *NJ* 2005/344 m.nt. E.J. Dommering.

EHRM 17 februari 2005, nrs. 42758/98 en 45558/99, ECLI:CE:ECHR:2005:0217JUD 004275898 (*K.A. en A.D. t. België*), *EHRC* 2005/38.

EHRM 9 juni 2005, nr. 55723/00 ECLI:CE:ECHR:2005:0609JUD005572300 (*Fadeyeva t. Rusland*), *EHRC* 2005/80, m.nt. H.L. Janssen.

EHRM 16 juni 2005, nr. 61603/00 (*Storck t. Duitsland*).

EHRM 20 oktober 2005, nr. 74989/01, ECLI:CE:ECHR:2005:1020JUD007498901 (*Ouranio Toxo e.a. t. Griekenland*), *EHRC* 2005/120.

EHRM (GK) 6 oktober 2005, nr. 74025/01, ECLI:CE:ECHR:2005:1006JUD007402501 (*Hirst t. het Verenigd Koninkrijk*), *EHRC* 2005/115 m.nt. J.L.W. Broeksteeg, *NTM|NJCM-bull.* 2006, p. 234 m.nt. H. Sackers.

EHRM 29 juni 2006, nr. 76900/01, ECLI:CE:ECHR:2006:0629JUD007690001 (*Öllinger t. Oostenrijk*), *EHRC* 2006/107.

EHRM 26 september 2006, nr. 12350/04, ECLI:CE:ECHR:2006:0926JUD001235004 (*Wainwright t. het Verenigd Koninkrijk*), *EHRC* 2006/130 m.nt. G. de Jonge.

EHRM (GK) 18 oktober 2006, nr. 46410/99, ECLI:CE:ECHR:2006:1018JUD004641099 (*Üner t. Nederland*).

EHRM 2 november 2006, nr. 59909/00, ECLI:CE:ECHR:2006:1102JUD005990900 (*Giacomelli t. Italië*), *AB* 2008/23 m.nt. T. Barkhuysen & M.L. van Emmerik.

EHRM 15 november 2007, nr. 12556/03, ECLI:CE:ECHR:2007:1115JUD001255603 (*Pfeifer t. Oostenrijk*), *EHRC* 2008/6 m.nt. J.H. Gerards.

EHRM 5 april 2007, nr. 18147/02, ECLI:CE:ECHR:2007:0405JUD001814702 (*Church of Scientology Moscow t. Rusland*).

EHRM 7 maart 2006, *Evans t. het Verenigd Koninkrijk*, nr. 6339/05, ECLI:CE:ECHR:2007:0410JUD000633905, *NJ* 2007/459 m.nt. J. de Boer, *EHRC* 2006/47 m.nt. E. Brems.

EHRM (GK) 10 april 2007, nr. 6339/05, ECLI:CE:ECHR:2007:0410JUD000633905 (*Evans t. het Verenigd Koninkrijk*), *NJ* 2007/459 m.nt. J. de Boer, *EHRC* 2007/73 m.nt. E. Brems.

EHRM 17 juli 2007, nr. 25691/04, ECLI:CE:ECHR:2007:0717JUD002569104 (*Bukta e.a. t. Hongarije*), *EHRC* 2007/11, m.nt. J.P. Loof, *NJ* 2007/631 m.nt. E.A. Alkema.

EHRM 11 september 2007, nr. 59894/00, ECLI:CE:ECHR:2007:0911JUD005989400 (*Bulgakov t. Oekraïne*).

EHRM 27 maart 2008, nr. 44009/05, ECLI:CE:ECHR:2010:0304JUD004400905 (*Shtukatarov t. Rusland*), *EHRC* 2008/74 m.nt. C. Forder.

EHRM 8 juli 2008, nr. 9103/04, ECLI:CE:ECHR:2008:0708JUD000910304 (*Georgische arbeiderspartij t. Georgië*), *EHRC* 2008/122 m.nt. J.L.W. Broeksteeg.

EHRM (GK) 8 juli 2008, nr. 10226/03, ECLI:CE:ECHR:2008:0708JUD001022603 (*Yumak en Sadak t. Turkije*), *EHRC* 2007/110 m.nt. J.L.W. Broeksteeg.

EHRM 7 oktober 2008, nr. 35228/03, ECLI:CE:ECHR:2008:1007JUD003522803 (*Bogumil t. Portugal*), *NJ* 2010/58 m.nt. F.C.B. van Wijmen.

EHRM (GK) 4 december 2008, nrs. 30562/04 en 30566/04, ECLI:CE:ECHR:2008:1204JUD003056204 (*S. en Marper t. het Verenigd Koninkrijk*), *EHRC* 2009/13 m.nt. B.J. Koops, *NJ* 2009/410 m.nt. E.A. Alkema.

EHRM 16 december 2008, nr. 23883/06, ECLI:CE:ECHR:2008:1216JUD002388306 (*Khurshid Mustafa en Tarzibachi t. Zweden*), *NJ* 2010/149, m.nt. E.A. Alkema, *AB* 2009/286, m.nt. T. Barkhuysen & M.L. van Emmerik, *EHRC* 2009/17, m.nt. J.H. Gerards.

EHRM 17 september 2009, nr. 13936/02 ECLI:CE:ECHR:2009:0917JUD001393602 (*Manole e.a. t. Moldavië*).

EHRM 28 mei 2009, nr. 26713/05, ECLI:CE:ECHR:2009:0528JUD002671305 (*Bigaeva t. Griekenland*), *EHRC* 2009/88 m.nt. S. Claessens.

EHRM 2 juni 2009, nr. 31675/04, ECLI:CE:ECHR:2009:0602JUD003167504 (*Codarcea t. Roemenië*), *EHRC* 2009/96 m.nt. E.H. Hulst.

EHRM (GK) 22 december 2009, nrs. 27996/06 en 34836/06, ECLI:CE:ECHR:2009:1222JUD002799606 (*Sejdić en Finci t. Bosnië en Herzegovina*), *EHRC* 2010/17 m.nt. J.H. Gerards.

EHRM 12 januari 2010, nr. 4158/05, ECLI:CE:ECHR:2010:0112JUD000415805 (*Gillan en Quinton t. het Verenigd Koninkrijk*), *EHRC* 2010/30 m.nt. P.B.C.D.F. van Sasse van Ysselt, *NJ* 2010/325 m.nt. E.J. Dommering.

EHRM 10 juni 2010, nr. 302/02, ECLI:CE:ECHR:2010:0610JUD000030202 (*Jehovah's Witnesses of Moscow t. Rusland*), *EHRC* 2010/89, m.nt. J.H. Gerards, *GJ* 2010/111 m.nt. A.C. Hendriks.

EHRM 2 september 2010, nr. 35623/05, ECLI:CE:ECHR:2010:0902JUD003562305 (*Üzun t. Duitsland*), *EHRC* 2010/123 m.nt. P. de Hert & J. van Caeneghem.

EHRM 14 september 2010, nrs. 2668/07 e.a. (*Dink t. Turkije*), *NJ* 2012/32 m.nt. E. Dommering, *EHRC* 2010/137 m.nt. R. van de Westelaken.

EHRM 19 oktober 2010, nr. 20999/04, ECLI:CE:ECHR:2010:1019JUD002099904 (*Özpinar t. Turkije*), *EHRC* 2011/5 m.nt. Barkhuysen & De Jong.

EHRM 21 oktober 2010, nr. 4916/07, 25924/08 en 14599/09, ECLI:CE:ECHR:2010:1021 JUD000491607 (*Alekseyev t. Rusland*), *EHRC* 2011/6, m.nt. J.P. Loof.

EHRM 23 november 2010, nrs. 60041/08 en 60054/08, ECLI:CE:ECHR:2010:1123JUD006004108 (*Greens e.a. t. het Verenigd Koninkrijk*), *EHRC* 2011/20, m.nt. R. de Lange, *NJ* 2012/285 m.nt. E.A. Alkema, *AB* 2011/123 m.nt. J. Uzman.

EHRM (GK) 16 december 2010, nr. 25579/05, ECLI:CE:ECHR:2010:1216JUD002557905 (*A., B. en C. t. Ierland*), *EHRC* 2011/40, m.nt. A.C. Hendriks & J.H. Gerards, *NJ* 2011/216 m.nt. E.A. Alkema, *GJ* 2011/36 m.nt. A.C. Hendriks.

EHRM 20 januari 2011, nr. 9300/07, ECLI:CE:ECHR:2011:0120JUD000930007 (*Herrmann t. Duitsland*), *EHRC* 2011/52 m.nt. J.H. Gerards.

EHRM 20 januari 2011, nr. 31322/07 (*Haas t. Zwitserland*), *EHRC* 2011/53 m.nt. G. den Hartogh, *NJ* 2002, 647 m.nt. J. Legemaate.

EHRM 22 februari 2011, nr. 6468/09, ECLI:CE:ECHR:2011:0222DEC000646809 (*Association Nouvelle des Boulogne Boyst. Frankrijk*), *EHRC* 2011/93 m.nt. M.J. Kanne.

EHRM (GK) 18 maart 2011, nr. 30814/06, ECLI:CE:ECHR:2011:0318JUD003081406 (*Lautsi e.a. t. Italië*), *EHRC* 2010/8, *NJ* 2011/588 m.nt. E.A. Alkema, *NJCM-Bull.* 2010, p. 294 m.nt. A.C. Hendriks & A.B. Terlouw.

EHRM 20 september 2011 (ontv.), nr. 48703/08, ECLI:CE:ECHR:2011:0920DEC004870308 (*Verein gegen Tierfabriken t. Zwitserland*).

EHRM 20 september 2011, nr. 14902/04, ECLI:CE:ECHR:2011:0920JUD001490204 (*OAO Neftyanaya Kompaniya Yukos t. Rusland*), *EHRC* 2011/160.

EHRM (GK) 3 november 2011, nr. 57813/00, ECLI:CE:ECHR:2011:1103JUD005781300 (*S.H. e.a. t. Oostenrijk*), *EHRC* 2012/38 m.nt. B. van Beers.

EHRM (GK) 7 februari 2012, nrs. 40660/08 en 60641/08, ECLI:CE:ECHR:2012:0207JUD004066008 (*Von Hannover t. Duitsland (nr. 2)*), *EHRC* 2012/72 m.nt. R. de Lange & J.H. Gerards, *NJ* 2013/250 m.nt. E.J. Dommering.

EHRM 10 mei 2012, nr. 7819/03, ECLI:CE:ECHR:2012:0510JUD000781903 (*Özgürlük Ve Dayanisma Partisi (ÖDP) t. Turkije*), *EHRC* 2012/144 m.nt. J.L.W. Broeksteeg.

EHRM 12 mei 2012, nr. 126/05, ECLI:CE:ECHR:2012:0522JUD000012605 (*Scoppola t. Italië nr. 3*), *EHRC* 2012/154 m.nt. R. de Lange, *NJ* 2013/373 m.nt. B.E.P. Myjer.

EHRM (GK) 7 juni 2012, nr. 38433/09 (*Centro Europa 7 S.r.l. en Di Stefano t. Italië*), *EHRC* 2012/188, m.nt. J. Wolswinkel.

EHRM 12 juni 2012 (ontv.), nr. 31098/08, ECLI:CE:ECHR:2012:0612DEC003109808 (*Hizb Ut-Tahrir e.a. t. Duitsland*), *EHRC* 2012/201 m.nt. P.E. de Morree.

EHRM 12 juni 2012, nrs. 26005/08 en 16160/08 (*Tátar en Fáber t. Hongarije*), ECLI:CE:ECHR:2012:0612JUD002600508, *EHRC* 2012/174, m.nt. J.H. Gerards.

EHRM 19 juli 2012, nr. 497/09, ECLI:CE:ECHR:2012:0719JUD000049709 (*Koch t. Duitsland*), *EHRC* 2012/220, *GJ* 2012/147 m.nt. Dorscheidt.

EHRM 2 oktober 2012 (ontv.), nr. 57942/10, ECLI:CE:ECHR:2012:1002DEC005794210 (*Rujak t. Kroatië*), *EHRC* 2013/21 m.nt. A. Nieuwenhuis.

EHRM 6 november 2012, nr. 47335/06, ECLI:CE:ECHR:2012:1106JUD004733506 (*Redfearn t. het Verenigd Koninkrijk*), *EHRC* 2013/29 m.nt. F. Laagland.

EHRM 15 januari 2013, nr. 8759/05, ECLI:CE:ECHR:2013:0115JUD000875905 (*Csoma t. Roemenië*), *EHRC* 2013/81 m.nt. A.C. Hendriks.

EHRM 14 maart 2013, nrs. 26261/05 en 26377/06, ECLI:CE:ECHR:2013:0314JUD002626105 (*Kasymakhunov en Saybatalov t. Rusland*), *EHRC* 2013/122 m.nt. P.E. de Morree.

EHRM 14 mei 2013, nr. 67810/10, ECLI:CE:ECHR:2014:0930JUD006781010 (*Gross t. Zwitserland*), *EHRC* 2013/152 m.nt. A.C. Hendriks.

EHRM 9 juli 2013, nr. 35943/10, ECLI:CE:ECHR:2013:0709JUD003594310 (*Vona t. Hongarije*), *EHRC* 2013/218 m.nt. P.E. de Morree, *NTM/NJCM-Bull.* 2014/41 m.nt. M.J. Kanne & J.L.W. Broeksteeg.

EHRM 16 juli 2013, nr. 1562/10, ECLI:CE:ECHR:2013:0716JUD000156210 (*Remuszenko t. Polen*).

EHRM 15 januari 2013, nrs. 48420/10 e.a., ECLI:CE:ECHR:2013:0115JUD004842010 (*Eweida e.a. t. het Verenigd Koninkrijk*), *EHRC* 2013/67 m.nt. J.H. Gerards.

EHRM 8 april 2014, nr. 31045/10, ECLI:CE:ECHR:2014:0408JUD003104510 (*The National Union of Rail, Maritime and Transport Workers t. het Verenigd Koninkrijk*), *EHRC* 2014/168 m.nt. F. Dorssemont; *JAR* 2014/128 m.nt. E. Koot-van der Putte.

EHRM (GK) 12 juni 2014, nr. 56030/07, ECLI:CE:ECHR:2014:0612JUD005603007 (*Fernández Martínez t. Spanje*), *EHRC* 2014/219 m.nt. A. Overbeeke.

EHRM (GK) 1 juli 2014, nr. 43835/11, ECLI:CE:ECHR:2014:0701JUD004383511 (*S.A.S. t. Frankrijk*), *EHRC* 2014/208 m.nt. P.B.C.D.F. van Sasse van Ysselt.

EHRM 7 oktober 2014, nr. 28490/02, ECLI:CE:ECHR:2014:1007JUD002849002 (*Begheluri e.a. t. Georgië*), *EHRC* 2015/10 m.nt. K. Henrard.

EHRM 6 november 2014, nr. 12927/13, ECLI:CE:ECHR:2014:1106JUD001292713 (*Dvořáček t. Tsjechië*), *EHRC* 2015/21 m.nt. A.C. Hendriks.

EHRM 10 maart 2015, nr. 14793/08, ECLI:CE:ECHR:2015:0310JUD001479308 (*Y.Y. t. Turkije*), *EHRC* 2015/106 m.nt. J.H. Gerards.

EHRM (GK) 5 juni 2015, nr. 46043/14, ECLI:CE:ECHR:2015:0605JUD004604314 (*Lambert t. Frankrijk*), *EHRC* 2015/171 m.nt. J.H. Gerards.

EHRM (GK) 16 juni 2015, nr. 64569/09 (*Delfi AS t. Estland*), ECLI:CE:ECHR:2015:0616JUD0064-56909, *EHRC* 2015/172 m.nt. B. van der Sloot, *NJ* 2016/457 m.nt. E.J. Dommering.

EHRM (GK) 4 december 2015, nr. 47143/06, ECLI:CE:ECHR:2015:1204JUD004714306 (*Roman Zakharov t. Rusland*), *EHRC* 2016/87 m.nt. M. Hagens, *NJ* 2017/185 m.nt. E.J. Dommering.

EHRM 5 januari 2016, nr. 74568/12, ECLI:CE:ECHR:2016:0105JUD007456812 (*Frumkin t. Rusland*), *EHRC* 2016/90 m.nt. R. de Jong.

EHRM 12 januari 2016, nr. 37138/14, ECLI:CE:ECHR:2016:0112JUD003713814 (*Szabó en Vissy t. Hongarije*).

EHRM (GK) 5 september 2017, nr. 61496/08, ECLI:CE:ECHR:2017:0905JUD006149608 (*Bărbulescu t. Roemenië*), *EHRC* 2018/3 m.nt. B.P. ter Haar, *JAR* 2017/259 m.nt. C.M. Jakimovicz.

EHRM 19 januari 2016, nr. 17526/10, ECLI:CE:ECHR:2016:0119JUD001752610 (*Gülcü t. Turkije*), *EHRC* 2016/77.

EHRM 29 maart 2016, nr. 16899/13, ECLI:CE:ECHR:2016:0329JUD001689913 (*Kocherov en Sergeyeva t. Rusland*), *EHRC* 2016/161.

EHRM. 18 oktober 2016, nr. 61838/10, ECLI:CE:ECHR:2016:1018JUD006183810 (*Vukota-Bojić t. Zwitserland*), *EHRC* 2017/33, m.nt. F.G. Laagland.

EHRM (GK) 26 april 2016, nr. 62649/10, ECLI:CE:ECHR:2016:0426JUD006264910 (*İzzettin Doğan e.a. t. Turkije*), *EHRC* 2016/167 m.nt. A.J. Overbeeke.

EHRM 22 maart 2016, nr. 23682/13, ECLI:CE:ECHR:2016:0322JUD002368213 (*Guberina t. Kroatië*), *EHRC* 2016/130 m.nt. L. Waddington, *AB* 2017/180 m.nt. H. Simon.

EHRM (GK) 24 mei 2016, nr. 38590/10, ECLI:CE:ECHR:2016:0524JUD003859010 (*Biao t. Denemarken*), *EHRC* 2016/209 m.nt. K. De Vries, *AB* 2017/179 m.nt. H. Simon.

EHRM 15 september 2016, nr. 44818/11 (*British Gurkha Welfare Society e.a. t. het Verenigd Koninkrijk*), *EHRC* 2016/101 m.nt. J.H. Gerards.

EHRM 8 november 2016, nr. 26126/07, ECLI:CE:ECHR:2016:1108JUD002612607 (*Naku t. Litouwen en Zweden*), *EHRC* 2017/14.

EHRM (GK) 8 november 2016, nr. 18030/11, ECLI:CE:ECHR:2016:1108JUD001803011 (*Magyar Helsinki Bizottság t. Hongarije*), *EHRC* 2017/36 m.nt. T. McGonagle.

EHRM (GK) 29 november 2016, nr. 34238/09 (*Lhermitte t. België*), ECLI:CE:ECHR:2016:1129JUD003423809, EHRC 2017/52 m.nt. K. Lemmens.

EHRM (GK) 24 januari 2017, nr. 25358/12, ECLI:CE:ECHR:2017:0124JUD002535812 (*Paradiso en Campanelli t. Italië*), *EHRC* 2017/85 m.nt. C. Mak.

EHRM 7 februari 2017, nr. 57818/09 en 14 andere, ECLI:CE:ECHR:2017:0207JUD 005781809 (*Lashmankin e.a. t. Rusland*), *EHRC* 2017/88 m.nt. B. Roorda.

EHRM 23 maart 2017, nr. 40524/08, ECLI:CE:ECHR:2017:0323JUD004052408 (*Genov t. Bulgarije*), *EHRC* 2017/108.

EHRM 28 maart 2017, nr. 25536/14, ECLI:CE:ECHR:2017:0328JUD002553614 (*Skorjanec t. Kroatië*), *EHRC* 2017/132 m.nt. K. Henrard.

EHRM 4 april 2017, nr. 35009/05, ECLI:CE:ECHR:2017:0404JUD003500905 (*Tek Gıda İş Sendikası t. Turkije*), *JAR* 2017/153.

EHRM 6 april 2017, nrs. 10138/11 en 3 andere, ECLI:CE:ECHR:2017:0406JUD001013811 (*Klein e.a. t. Duitsland*), *EHRC* 2017/127 m.nt. M.R.T. Pauwels.

EHRM 27 juni 2017, nr. 39793/17, ECLI:CE:ECHR:2017:0627DEC003979317 (*Gard e.a. t. het Verenigd Koninkrijk*), *EHRC* 2017/193 m.nt. J.H. Gerards.

EHRM 20 juni 2017, nrs. 67667/09 en 2 andere, ECLI:CE:ECHR:2017:0620JUD006766709 (*Bayev e.a. t. Rusland*), *EHRC* 2017/158 m.nt. J.H. Gerards.

EHRM 18 mei 2017, nr. 40927/05, ECLI:CE:ECHR:2017:0518JUD004092705 (*Boze t. Letland*).

EHRM 24 oktober 2017, nrs. 57818/10, 57822/10, 57825/10, 57827/10 en 57829/10, ECLI:CE:ECHR:2017:1024JUD005781810 (*Tibet Mentes t. Turkije*), *EHRC* 2018/10.

EHRM 31 oktober 2017, nr. 22767/08, ECLI:CE:ECHR:2017:1031JUD002276708 (*Dragoş Ioan Rusu t. Roemenië*), *EHRC* 2018/13 m.nt. D.A.G. van Toor.

EHRM 21 november 2017, nr. 47056/11, ECLI:CE:ECHR:2017:1121JUD004705611 (*Panyshkiny t. Rusland*).

EHRM 28 november 2017, nr. 70838/13, ECLI:CE:ECHR:2017:1128JUD007083813 (*Antović en Mirković t. Montenegro*), *JAR* 2018/20.

EHRM 5 december 2017, nr. 57792/15, ECLI:CE:ECHR:2017:1205JUD005779215 (*Hamidovic t. Bosnië-Herzegovina*).

EHRM 9 januari 2018, nrs. 1874/13 en 8567/13, ECLI:CE:ECHR:2018:0109JUD000187413 (*López Ribalda e.a. t. Spanje*), *JAR* 2018/56 m.nt. I.J. de Laat.

EHRM 13 februari 2018, nr. 61064/10, ECLI:CE:ECHR:2018:0213JUD006106410 (*Ivashchenko t. Rusland*).

EHRM 22 februari 2018, nr. 72562/10, ECLI:CE:ECHR:2018:0222JUD007256210 (*Alpha Doryforiki Tileorasi Anonymi Etairia t. Griekenland*).

EHRM 22 februari 2018, nr. 588/13, ECLI:CE:ECHR:2018:0222JUD000058813 (*Libert t. Frankrijk*).

Europese Commissie voor de Rechten van de Mens

ECieRM 30 mei 1975, nrs. 6745/74 en 6746/74, *DR* 110, p. 113 (*W, X, Y en Z t. België*).

ECieRM 8 mei 1976 nr. 6825/74, 5 *DR* 86, p. 87 (*Commissie X t. IJsland*).

ECieRM 10 juli 1978, nr. 8257, *DR* 13, p. 248 (*X t. Zwitserland*).

ECieRM 15 december 1983, nr. 10358/83, *DR* 37, p. 142. (*C. t. het Verenigd Koninkrijk*).

Hoge Raad

HR 9 januari 1987, *NJ* 1987/928 (*Edamse bijstandsmoeder*).

HR 15 april 1994, *NJ* 1994/608 (*Valkenhorst*).

HR 6 januari 1995, *NJ* 1995/422 m.nt. E.J. Dommering (*Parool*).

HR 19 december 1995, *NJ* 1996/249.

HR maart 1996, *NJ* 1997/86.

HR 21 december 2012, *NJ* 2011/23.

HR 18 april 2014, *NJ* 2014/507.

Afdeling Bestuursrechtspraak Raad van State

ABRvS 28 augustus 1995, *AB* 1996/204.

ABRvS 10 augustus 1999, *AB* 2000/168.

ABRvS 9 januari 2008, *GJ* 2008/37 m.nt. Y.M. Drewes & A.C. Hendriks.

ABRvS 17 mei 2017, *Computerrecht* 2017/256, m.nt. B.M.A. van Eck.

Centrale Raad van Beroep

CRvB 3 mei 2002, *AB* 2002/346.

Gerechtshof Amsterdam

Hof Amsterdam 8 januari 1998, *NJ* 2000/152.

Rechtbank

Rb Groningen 22 januari 2003, *NJ* 2003/169.

Vz Rb Utrecht 25 mei 2007, *NJF* 2007/334.

Rb Amsterdam, 31 mei 2017, ECLI:NL:RBAMS:2017:3772.

College voor de Rechten van de Mens

College voor de Rechten van de Mens van 11 december 2017, oordeel 2017-145.

Overig

Supreme Court Wisconsin, *State v. Loomis*, 881 N.W.2d 749 (Wis. 2016).