M. Vetzo & J.H. Gerards[1]

Algoritme-gedreven technologieën en grondrechten

Computerrecht 2019/3

De opkomst van algoritme-gedreven technologieën als Big Data-analyse, 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 artikel wordt daarom in kaart gebracht wat de (potentiële) knelpunten zijn waar het gaat om de impact van algoritme-gedreven technologieën op vrijheidsrechten, gelijkheidsrechten, privacyrechten en procedurele rechten.

1. Inleiding

Dat nieuwe technologieën op gespannen voet kunnen staan met grondrechten, is op veel plaatsen al beschreven.[2] Met het voortschrijden van algoritme-gedreven technologische ontwikkelingen als Big Data-analyses, het Internet of Things (IoT) en Kunstmatige Intelligentie (KI) doemen bovendien potentiële nieuwe grondrechtelijke knelpunten op. Tot voor kort ontbrak een specifiek op Nederland gerichte, juridische en systematische studie naar de gevolgen van deze technologieën voor de bescherming van andere grondrechten dan informationele privacy en gegevensbescherming. Om dit hiaat te vullen hebben wij op verzoek van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties geïnventariseerd op welke manier de genoemde drie technologieën de grondrechten in Nederland mogelijk aantasten.[3] Daarbij concentreert ons onderzoek zich op de effecten van deze drie technologieën, en in het bijzonder op de grote gemeenschappelijke deler hiervan: het gebruik van algoritmes. De vraag is daarbij welke knelpunten deze technologieën opleveren voor vier clusters van grondrechten: (1) 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); (2) gelijkheidsrechten (het recht op gelijke behandeling en non-discriminatie); (3) 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); en (4) procedurele rechten: het recht op een eerlijk proces en een effectief rechtsmiddel. Het recht op persoonsgegevensbescherming is in dit onderzoek buiten beschouwing gelaten. De afgelopen jaren is er al veel aandacht geweest voor de impact van de onderzochte technologieën op de bescherming van persoonsgegevens, vooral omdat ze allemaal werken met (grote hoeveelheden) data, waaronder persoonsgegevens. Die aandacht heeft veel te maken met de inwerkingtreding van de Algemene Verordening Gegevensbescherming, die tal van bepalingen bevat die van belang zijn voor de manier waarop persoonsgegevens worden verwerkt. Voor andere grondrechten is er vaak wat minder aandacht geweest. Door daarop te focussen en daarmee een iets ander perspectief te kiezen dan vaak gebeurt, helpt dit onderzoek om de juridische en maatschappelijke discussie te verbreden.

Hierna presenteren we de belangrijkste bevindingen van onze studie.[4] Daarbij geven we eerst een korte introductie op de drie technologieën die in het onderzoek centraal staan en op het gebruik van algoritmes (paragraaf 2). Vervolgens schetsen we per grondrechtencluster het grondrechtelijk kader en laten we zien waar algoritme-gedreven technologieën kunnen leiden tot knelpunten (paragraaf 3). In de afsluitende paragraaf 4 bezien we deze grondrechtelijke knelpunten in samenhang. Daarbij geven we ook een aanzet voor de beantwoording van de vraag waar zich de voornaamste grondrechtelijke problemen voordoen.

2. Big Data, Internet of Things, Kunstmatige Intelligentie en algoritmes

2.1 *Big Data, Internet of Things en Kunstmatige Intelligentie*

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.[5] 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 IoT en KI zijn belangrijke krachten achter van dit proces van digitalisering. Deze drie

1 Max Vetzo is student in de Legal Research Master van de Universiteit Utrecht. Janneke Gerards is hoogleraar fundamentele rechten bij de Universiteit Utrecht; zij is verbonden aan het strategisch programma Instituties voor Open Samenlevingen en het Montaigne Centrum voor Rechtsstaat en Rechtspleging.

2 Zie reeds *Rapport Commissie Grondrechten in het digitale tijdperk*, Den Haag 2000; recenter R. van Est & J. Gerritsen (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; F.A. Raso e.a., *Artificial Intelligence & Human Rights: Opportunities and Risks*, Harvard 2018(https://cyber.harvard.edu/publication/2018/artificial-intelligence-human-rights); M. Latonero, *Governing Artificial Intelligence: Upholding Human Rights and Dignity*, Data & Society 2018.

3 Mogelijk zijn er ook positieve effecten op de grondrechten, maar die zijn in deze knelpuntenanalyse niet verder onderzocht; zie wel bijv. Raso e.a. 2018 (noot 2).

4 De veel uitgebreidere versie is te vinden in M.J. Vetzo, J.H. Gerards & R. Nehmelman, *Algoritmes en grondrechten*, Den Haag: Boom 2018 (www.rijksoverheid.nl/documenten/rapporten/2018/03/01/algoritmes-en-grondrechten).

5 L. Kool e.a., *Opwaarderen. Borgen van publieke waarden in de digitale samenleving*, Den Haag: Rathenau Instituut 2017.

fenomenen hebben aanzienlijke invloed op het functioneren van overheden, bedrijven en het dagelijks leven van vele mensen.

Allereerst heeft een reeks technologische ontwikkelingen ertoe geleid dat zeer grote hoeveelheden data kunnen worden gegenereerd, opgeslagen en verwerkt: Big Data. Overheden en bedrijven zijn steeds beter in staat om uit deze grote hoeveelheid ongestructureerde, zeer gevarieerde en vaak 'real-time' gegevens relevante informatie te destilleren. Deze informatie kan vervolgens worden gebruikt ten behoeve van (automatische) besluitvorming. Dit proces van dataverzameling, analyse en gebruik wordt aangeduid als het Big Data-proces.[6]

Een tweede fenomeen, het IoT, ziet op de ontwikkeling waarbij steeds meer 'alledaagse' apparaten met het Internet verbonden raken, zoals verlichting of een verwarming die op afstand kunnen worden aangezet, een smartwatch die de hartslag registreert, of een koelkast die bijhoudt welke producten moeten worden bijgekocht.[7] Dit soort apparaten kan data waarnemen en doorgeven en draagt zo bij aan een vergaande digitalisering van de fysieke wereld.

Ten slotte richt KI zich op computers en apparaten die intelligentie kunnen nabootsen; het is een verzamelterm voor een veelheid aan technologieën.[8] Een belangrijk deelgebied van KI is 'Machine Learning'. Machine Learning-technieken stellen computers in staat zelf te 'leren' om taken uit te voeren, zonder daartoe expliciet geprogrammeerd te zijn. In een geavanceerde vorm van Machine Learning, 'Deep Learning', wordt gebruikgemaakt van neurale netwerken die zijn gemodelleerd naar het menselijk brein. Via deze gelaagde analyses kunnen complexe, verborgen verbanden in datasets worden ontdekt, en daarmee kan nieuwe kennis worden gegenereerd. KI kan op allerlei manieren worden toegepast, bijvoorbeeld in expertsystemen die, al redenerend, verkregen kennis op nieuwe feiten kunnen toepassen, of in robots die 'intelligente' handelingen uitvoeren.

Deze korte beschrijving laat zien dat Big Data, het IoT en KI samenhangende fenomenen zijn. Het IoT draagt, samen met andere technologieën, bij aan het beschikbaar maken van Big Data.[9] Het Big Data-proces richt zich op het destilleren van relevante informatie uit al deze data. De centrale positie van KI verdient daarbij bijzondere aandacht. Hoewel in het bovenstaande de zelfstandige rol van KI wordt benadrukt, kan KI ook worden beschouwd als een technologie ten behoeve van het functioneren van (onder meer) Big Data en het IoT. Zo wordt KI ingezet voor complexe Big Data-analyses en de analyse van door het IoT verzamelde informatie.[10] In zoverre vormt KI een onderdeel van Big Data en het IoT.

2.2 *Algoritmes als verbindende factor*

Algoritmes vormen de cruciale verbindende factor tussen Big Data, het IoT en KI. De primaire bouwsteen van KI wordt gevormd door algoritmes. Deze algoritmes stellen computers, robots en apparaten in staat zich intelligent te gedragen en zelfs om zelfstandig te leren. Algoritmes vormen daarmee de basis van slimme technologie.[11] De omvang en ongeordendheid van Big Data maakt dat het zoeken naar relevante patronen neerkomt op het zoeken van een naald in een hooiberg. Algoritmes maken het mogelijk om zinvolle informatie te destilleren uit de grote hoeveelheden data die mensen en apparaten genereren.[12] Ook voor het functioneren van het IoT is de algoritmische analyse van de grote hoeveelheid verzamelde data en snelle terugkoppeling hiervan aan apparaten of gebruikers essentieel.[13] Algoritmes maken het mogelijk om de door sensoren geregistreerde informatie te analyseren op een zodanige manier dat die bruikbaar wordt voor een applicatie.

Het functioneren van de drie hier bestudeerde technologieën hangt dus mede af van de algoritmes die worden gebruikt. Eenvoudig gezegd bestaan algoritmes uit een set instructies die worden ingezet voor het oplossen van bepaalde problemen. Deze instructies worden meegegeven aan computers, waarvan de rekenkracht vele malen sneller en groter is dan die van mensen. De set instructies maakt het mogelijk om inputdata om te zetten naar outputdata ten behoeve van het oplossen van het probleem.[14] De output van het algoritme vormt dus de oplossing voor het gegeven probleem. Zo beschouwd zijn algoritmes niet meer dan een recept; een set aan instructies.[15] Inderdaad zijn sommige algoritmes eenvoudig, bijvoorbeeld omdat ze een basale 'als-dan'-structuur hebben: als aan instructie x is voldaan, volgt gevolg y. Andere algoritmes kunnen als 'slim' worden aangeduid. Door technologische ontwikkelingen, met name op het terrein van KI en Machine Learning, zijn algoritmes in toenemende mate in staat om te leren op basis van de output die zij zelf genereren. Deze zelflerende algoritmes kunnen zich automatisch aanpassen aan die output en zo complexe verbanden in data ontdekken. De in deze studie beschreven algoritmes zijn vooral dergelijke slimme algoritmes, omdat deze – beter dan hun niet-zelflerende tegen-

6 Wetenschappelijke Raad voor het Regeringsbeleid, *Big Data in een vrije en veilige samenleving* (rapport nr. 95), Den Haag 2016 (www.wrr.nl/onderwerpen/big-data-privacy-en-veiligheid/documenten/rapporten/2016/04/28/big-data-in-een-vrije-en-veilige-samenleving), p. 33-48.

7 Zie verder bijv. International Telecommunication Union, *Overview of the Internet of Things*, 2012 (www.itu.int/ITU-Y/recommendations/rec.aspx?rec=Y.2060).

8 Zie o.m. S.J. Russell & P. Norvig, *Artifical Intelligence. A Modern Approach*, New York: Pearson Education 2010.

9 S. Poudel, 'Internet of Things: underlying technologies, interoperability, and threats to privacy and security', *Berkeley Technology Law Journal* 2016, p. 1005-1006.

10 Vgl. over de relatie tussen Big Data en KI, UK Information Commissioner, *Big data, artificial intelligence, machine learning and data protection*, 4 september 2017 (www.ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf), p. 8.

11 Zie hierover in het algemeen Russel & Norvig 2010 (noot 8).

12 A. Vedder & L. Naudts, 'Accountability for the use of algorithms in a big data environment', *International Review of Law, Computers & Technology* 2017, p. 207.

13 Poudel 2016 (noot 9), p. 1007-1008.

14 Zie o.a. N. Diakopoulos, 'Algorithmic Accountability', *Digital Journalism* 2015, p. 400.

15 M. Hildebrandt, 'The New Imbroglio. Living with Machine Algorithms', in: L. Janssens (red.), *The Art of Ethics in the Information Society*, Amsterdam: Amsterdam University Press 2016, p. 56.

hangers – bij uitstek geschikt zijn voor het verrichten van complexe (voorspellende) analyses.

2.3 *Bijzondere kenmerken van algoritmes*

Voor een goed begrip van de impact van algoritmes op grondrechten, is het van belang om in te zien dat algoritmes menselijke, niet-neutrale en ondoorzichtige constructen zijn. Ze zijn menselijk in die zin dat mensen verantwoordelijk zijn voor het programmeren en (waar nodig) trainen van algoritmes. Het belang van de door mensen gemaakte keuzes in de ontwerp- en ontwikkelfase kan nauwelijks worden onderschat, onder meer doordat de in deze fase gemaakte keuzes doorwerken in de data-analyses en in de gegenereerde output.[16]

Hoewel veel mensen algoritmes associëren met objectiviteit en neutraliteit, kunnen algoritmes op allerlei manieren blijk geven van subjectiviteit en 'bias'.[17] In de ontwerp- en trainingsfase kunnen waarden of vooroordelen van programmeurs of opdrachtgevers van programmeurs bijvoorbeeld worden ingebed in algoritmes.[18] Daarnaast kunnen datasets of oefendata waarmee een algoritme werkt, *biases* bevatten die bepalend zijn voor de uitkomsten van het algoritme.[19] In dit verband is ook van belang dat algoritmes bij Big Data-analyses geen inzicht bieden in causale verbanden, maar alleen wijzen op correlaties. Deze correlaties kunnen nuttig en waardevol zijn, maar ze kunnen ook op toeval berusten. Het gebruik van een algoritme leidt in die gevallen gemakkelijk tot redeneerfouten.

Waar eenvoudige algoritmes relatief transparant zijn, worden slimme algoritmes gekenmerkt door ondoorzichtigheid. Deze ondoorzichtigheid hangt samen met hun complexiteit. Algoritmes zijn in programmeertaal vastgelegde technische constructen, die worden gekoppeld aan omvangrijke, veranderlijke datasets. Dat maakt dat het doorgronden van het algoritme en de omgeving waarin dit algoritme fungeert zowel technologisch als contextueel complex is. Algoritmes worden daardoor vaak gezien als een 'black box':[20] de input en output van het algoritme zijn bekend, maar hoe het tussenliggende proces functioneert is moeilijk te doorgronden.[21] Met andere woorden: de uitkomst van een algoritme is (*ex ante*) lastig te voorspellen en (*ex post*) lastig uit te leggen. De ondoorzichtigheid van algoritmes wordt versterkt doordat algoritmes vaak geheim worden gehouden. Om commerciële of veiligheidsredenen kiezen bedrijven en overheden er regelmatig voor om de algoritmes die ten grondslag liggen aan besluitvorming niet openbaar te maken.[22]

3. Grondrechtelijke knelpunten bij algoritme-gedreven technologieën

De alomtegenwoordigheid van algoritme-gedreven technologieën en de veelheid aan concrete toepassingen, gecombineerd met de inherente kenmerken van algoritmes, roept de vraag op welke invloed deze technologieën hebben op de bescherming van grondrechten. Hierna wordt die invloed inzichtelijk gemaakt door voor vier grondrechtenclusters (privacyrechten, gelijkheidsrechten, vrijheidsrechten en procedurerechten) op hoofdlijnen – en voor zover relevant – weer te geven welke waarborgen deze grondrechten beogen te bieden, en op welke manier de bestudeerde technologieën op deze grondrechten kunnen inwerken.

3.1 *Privacyrechten*

3.1.1 *Grondrechtelijk kader*

Het recht op privacy, dat nauw verband houdt met persoonlijke autonomie en menselijke waardigheid, laat zich lastig definiëren.[23] In een moderne formulering behelst privacy het recht van een individu om 'zichzelf' te zijn en te doen en laten wat hij wil, zonder bemoeienis van de overheid of derden. Dit recht om zichzelf te zijn heeft iemand zowel thuis als in de publieke of digitale ruimte. In de afgelopen decennia heeft een nadere omlijning plaatsgevonden aan de hand van de talrijke codificaties die aan de privacyrechten zijn gegeven, zoals artikel 10 Grondwet, artikel 8 Europees Verdrag voor de Rechten van de Mens (EVRM) en artikel 7 Handvest van de Grondrechten van de Europese Unie (Hv). Uit deze specificaties blijkt dat een ruime variatie aan privacyrechten wordt gegarandeerd. Het gaat dan allereerst 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 eigendommen naar eigen inzicht te kunnen gebruiken.[24] In de tweede plaats is er een aantal rechten dat samenhangt met de persoonlijke identiteit, zoals het naamrecht en het recht de eigen identiteit te bepalen.[25] In verband hiermee is het belang erkend van de ontwikkeling van iemands sociale identiteit en het recht om relaties aan te gaan met anderen.[26] Ook het recht op lichamelijke en geestelijke integriteit

16 Diakopoulos 2015 (noot 14), p. 402.

17 T. Gillespie, 'The Relevance of Algorithms', in: T. Gillespie e.a. (red.), *Media technologies: Essays on communication, materiality, and society*, Cambridge MA: MIT Press 2014, p. 179.

18 D.K. Citron & F. Pasquale, 'The Scored Society: Due Process for Automated Predictions', *Washington Law Review* 2014, p. 4.

19 Zie nader S. Barocas & A.D. Selbst, 'Big Data's Disparate Impact', *California Law Review* 2016, p. 671-732.

20 F. Pasquale, *The Black Box Society. The Secret Algorithms That Control Money and Information*, Cambridge (MAS): Harvard University Press 2015.

21 A. Rouvroy, *'Of Data and Men': Fundamental Rights and Liberties in a World of Big Data*, Straatsburg: Raad van Europa 2016, p. 12 (www.researchportal.unamur.be/en/publications/of-data-and-men-fundamental-rights-and-liberties-in-a-world-of-bi).

22 Hierover J.A. Kroll e.a., 'Accountable Algorithms', *University of Pennsylvania Law Review* 2017, p. 657-658.

23 *Kamerstukken II* 1975/76, 13782, 3, p. 41.

24 Zie ook B.J. Koops e.a., 'A Typology of Privacy', 38 *University of Pennsylvania International Law Review* 2017, par. 4.3.

25 Zie nader bijv. 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) 2015, C.3.

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

is erkend als onderdeel van het privéleven.[27] Tot slot heeft een nauw met persoonlijke autonomie verwant recht een aparte plaats gekregen in de grondrechtencodificaties, namelijk de gewetensvrijheid en de vrijheid om een mening te koesteren.[28]

Deze privacyrechten zijn primair negatief geformuleerde afweerrechten: de staat hoort zich niet te mengen in, bijvoorbeeld, de individuele keuzevrijheid, zonder dat daarvoor een goede rechtvaardiging bestaat. Aan de rechtvaardiging voor zo'n inmenging worden formele en materiële eisen gesteld, met name in de rechtspraak van het Europees Hof voor de Rechten van de Mens (EHRM) en Hof van Justitie van de EU (HvJ).[29] Deze eisen zien onder meer op de noodzaak van een wettelijke grondslag, een legitieme doelstelling en een redelijke afweging tussen de betrokken belangen.
Naast de taak om zich te onthouden van ongerechtvaardigde inmengingen, heeft de staat volgens de rechtspraak tal van positieve verplichtingen om de verschillende grondrechten actief te beschermen of om bepaalde voorwaarden te creëren om de uitoefening van een grondrecht effectief mogelijk te maken.[30] Door deze positieve verplichtingen hebben de privacyrechten ook een sterke, zij het indirecte, horizontale werking. Een kenmerkend voorbeeld is dat het EHRM weliswaar toelaat dat werkgevers inbreuk maken op de privacy van hun werknemers, bijvoorbeeld door inzage te krijgen in hun e-mailgebruik, maar het Hof vereist dan wel dat nationale regelgeving wordt aangenomen om de zorgvuldigheid van dit toezicht te reguleren.[31] Ook de nationale rechter – inclusief de burgerlijke rechter in privacyrechtelijke geschillen – heeft volgens het EHRM een positieve verplichting om in overeenstemming met het EVRM te oordelen.[32]

3.1.2 *Privacyrechtelijke knelpunten*

Bij de uitoefening van de hierboven kort besproken privacyrechten kan een veelheid van grondrechtelijke knelpunten ontstaan als gevolg van algoritme-gedreven technologieën. Dit vindt zijn verklaring in de ruime reikwijdte van de privacyrechten, in combinatie met het gedetailleerde beeld dat met behulp van deze technologieën verkregen kan worden van het leven van burgers. De knelpunten bij de uitoefening van privacyrechten kunnen zich voordoen in zowel verticale relaties (overheid-burger) als horizontale (private) verhoudingen. Op hoofdlijnen kunnen de volgende (potentiële) knelpunten van algoritmegedreven technologieën worden geïdentificeerd.

Allereerst kan uit rechtspraak van het EHRM 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.[33] Deze inbreuken kunnen zich voordoen in de privéomgeving, maar ook in publieke ruimtes,[34] bijvoorbeeld in *smart cities* waarin op grote schaal gebruik wordt gemaakt van IoT-apparaten die *real-time* data verzamelen om het welzijn en de veiligheid in een stad te monitoren. Bovendien vindt deze 'dataveillance' niet alleen plaats door de overheid, maar ook door bedrijven. De inzet van KI of het IoT op de werkvloer kan bijvoorbeeld raken aan het recht op privacy van werknemers.[35] Dit soort inbreuken op de privacy moet voldoen aan de beperkingseisen die door de relevante grondrechtenbepalingen worden gesteld, of die naar analogie daarvan in horizontale gevallen kunnen worden toegepast. Daarbij verdienen met name de beperkingseisen van artikel 8 EVRM aandacht, bijvoorbeeld in het kader van de inzet van politiële datamining of het gebruik van het IoT ten behoeve van de opsporing.[36] In het bijzonder moet regelgeving (of interne bedrijfsregelingen) voldoende duidelijk zijn verwoord om de consequenties van het gebruik van bepaalde technologieën te kunnen inschatten, moeten waarborgen worden geboden tegen willekeurig gebruik hiervan, en moet adequate toegang tot rechtsbescherming worden geboden.[37] Meer algemeen laat dit zien dat alle inbreuken op het recht op privacy die worden veroorzaakt door Big Data, KI en het IoT een wettelijke grondslag nodig hebben. Als daarbij gebruik wordt gemaakt van de mogelijkheid van delegatie aan decentrale overheden, bijvoorbeeld om socialezekerheidsregelgeving uit te voeren, dan moet de regeling die in de beperking voorziet bovendien voldoende gespecificeerd zijn, dat wil zeggen uitdrukkelijk geschreven voor de beperking van het recht op privacy.[38]

Het voortdurend verzamelen en analyseren van data door middel van algoritmes kan ook meer abstracte effecten hebben voor privacyrechten. In het bijzonder kunnen algoritme-gedreven technologieën leiden tot 'chilling effects', in

27 Zie reeds EHRM 26 maart 1985, nr. 8978/80, ECLI:CE:ECHR:1985:0326JUD000897880 (*X. en Y./Nederland*), *NJ* 1985/525, m.nt. E.A. Alkema, par. 22.

28 Nader bijv. 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.

29 Zie nader J.H. Gerards, *EVRM – Algemene beginselen*, Den Haag: Sdu 2011.

30 Zie over het concept 'positieve verplichtingen' nader Gerards 2011 (noot 29), p. 229 e.v.; 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; M.P. Beijer, *The Limits of Fundamental Rights Protection by the EU. The Scope for the Development of Positive Obligations*, Antwerpen: Intersentia 2017.

31 Zie EHRM (GK) 5 september 2017, nr. 61496/08, ECLI:CE:ECHR:2017:0905JUD006149608 (*Bărbulescu/Roemenië*), *EHRC* 2018/3, m.nt. B.P. ter Haar.

32 Zie bijv. EHRM (GK) 7 februari 2012, nrs. 40660/08 en 60641/08, ECLI:CE:ECHR:2012:0207JUD004066008 (*Von Hannover/Duitsland (nr. 2)*), *EHRC* 2012/72, m.nt. R. de Lange & J.H. Gerards, *NJ* 2013/250, m.nt. E.J. Dommering.

33 Zie bijv. EHRM 12 januari 2016, nr. 37138/14, ECLI:CE:ECHR:2016:0112JUD003713814 (*Szabó en Vissy/Hongarije*), par. 70; zie ook 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. de Koning, *NJ* 2016/446, m.nt. E.J. Dommering, par. 27.

34 EHRM 25 september 2001, nr. 44787/98, ECLI:CE:ECHR:2001:0925JUD004478798 (*P.G. en J.H./Het Verenigd Koninkrijk*), *NJ* 2003/670, m.nt. E.J. Dommering, par. 56-57.

35 Zie EHRM *Bărbulescu/Roemenië* (noot 31).

36 Zie bijv. S. Brinkhoff, 'Datamining in een veranderende wereld van opsporing en vervolging', *Tijdschrift voor Bijzonder Strafrecht en Handhaving* 2017, p. 224-227.

37 Zie nader J.H. Gerards, *General principles of the European Convention on Human Rights Law*, Cambridge: Cambridge University Press, te verschijnen (2019), par. 8.7.

38 Zie, specifiek ten aanzien van artikel 10, lid 1 Grondwet, ABRvS 28 augustus 1995, *AB* 1996/204 (*Drugspand Venlo*).

die zin dat individuen 'gewenst' gedrag gaan vertonen in de wetenschap dat zij constant in de gaten worden gehouden.[39] Het op deze wijze sturen van het denken en handelen van personen raakt aan het recht op persoonlijke autonomie. 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. Nauw verband hiermee houdt het 'recht om vergeten te worden'. Door het langdurige 'geheugen' van veel technologische toepassingen en door het vermogen om verbanden te leggen tussen data, kan het recht om de eigen identiteit vorm te geven in het geding komen.[40] Uiteraard zijn er beperkingen mogelijk van deze rechten, maar die moeten steeds voldoen aan de formele en materiële beperkingseisen.

Ook de inzet van KI, bijvoorbeeld in de vorm van robots, kan leiden tot moeilijkheden bij het effectueren van het recht op privacy. Het gaat dan vooral om relationele privacy, bijvoorbeeld in het kader van de zorg voor hulpbehoevenden. De vrees is dat personen worden 'ontmenselijkt' als zij geen (of veel minder) contact meer hebben met 'echte' mensen.[41] Dat raakt aan het recht om de eigen persoonlijkheid en identiteit vorm te geven door het aangaan van relaties met andere mensen.

3.2 *Gelijkheidsrechten*

3.2.1 *Grondrechtelijk kader*

Het recht op gelijke behandeling en non-discriminatie is een complex recht, dat onder meer is gecodificeerd in artikel 1 Grondwet, artikel 14 EVRM, artikel 20 en 21 Hv en bijzondere gelijkebehandelingswetgeving. Oneindige gelijke behandeling is daarbij niet het streven; vooropstaat dat het *zonder goede rechtvaardiging* ongelijk of juist gelijk behandelen van personen of groepen moet worden voorkomen.
Aangenomen wordt meestal dat een benadeling gerechtvaardigd is in twee situaties.[42] Allereerst is dit zo wanneer sprake is van een benadeling ten opzichte van elkaar van *onvergelijkbare gevallen of groepen*. 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 relevant verschillend zijn. In de tweede plaats kan de beoordeling van de redelijkheid van een benadeling worden onderzocht of er een *objectieve en redelijke rechtvaardiging* bestaat voor die benadeling, waarbij wordt onderzocht of de grond van onderscheid voldoende objectief, neutraal en redelijk is en het doel van het onderscheid in een proportionele relatie staat tot de benadeling die er het gevolg van is. Daarbij wordt algemeen aangenomen dat ongelijke behandeling op sommige gronden a priori 'verdacht' is.[43] Dat is vooral zo 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, of als een benadeling wordt gebaseerd op persoonskenmerken die objectief gezien irrelevant zijn voor iemands dagelijkse functioneren in de samenleving. Is een onderscheid rechtstreeks gebaseerd op een van deze verdachte gronden, dan is sprake van 'directe' discriminatie. Een verdachte grond (bijvoorbeeld etniciteit) is dan het enige of in ieder geval doorslaggevende motief voor een benadeling. Discriminatie kan echter ook indirect zijn. In dat geval is een benadeling niet rechtstreeks gebaseerd op een verdachte grond, maar is het effect van een 'neutrale' regeling of beslissing wel een benadeling van de leden van de groep die zo'n verdachte grond kenmerkt.

3.2.2 *Discriminatieknelpunten*

De opkomst van algoritme-gedreven technologieën heeft geleid tot een forse toename van de mogelijkheden tot differentiatie tussen (groepen) personen door de overheid en private actoren. Dergelijke differentiatie is vanuit grondrechtelijk perspectief problematisch als die leidt tot ongerechtvaardigd onderscheid. Op hoofdlijnen doen zich verschillende knelpunten voor.

Allereerst kunnen de in paragraaf 2 omschreven inherente ondoorzichtigheid en complexiteit van algoritmes maken dat het voor mensen onduidelijk is of sprake is van ongerechtvaardigde ongelijke behandeling. Algoritmische discriminatie, die bijvoorbeeld ontstaat door een *bias* in de data en/of in de gebruikte algoritmes, kan niet altijd eenvoudig worden ontdekt en gecontroleerd.[44] Dit bemoeilijkt de zichtbaarheid en het bewijs van ongelijke behandeling.[45] Dit geldt in nog sterkere mate als algoritmische discriminatie intentioneel is gemaskeerd.[46] Dat is problematisch, omdat het onder meer in het strafrecht van belang is of sprake is van opzettelijke discriminatie.[47]
Bij toepassing van Big Data-analyse gaat het altijd om een veelheid aan factoren die resulteert in onderscheid tussen

39 Zie bijvoorbeeld F.J. Zuiderveen Borgesius, *Improving privacy protection in the area of behavioural targeting* (diss. Amsterdam UvA), Alphen aan den Rijn: Kluwer Law International 2014, p. 111.
40 Zie over de technologische complexiteit van de effectuering van het recht om vergeten te worden, E.F. Villaronga e.a., 'Humans forget, machines remember: Artificial Intelligence and the Right to Be Forgotten', *Computer Law and Security Review* 2017, p. 1-10.
41 Van Est & Gerritsen 2017 (noot 2), p. 25.
42 Nader J.H. Gerards, *Rechterlijke toetsing aan het gelijkheidsbeginsel. Een rechtsvergelijkend onderzoek naar een algemeen toetsingsmodel* (diss. Maastricht), Den Haag: Sdu 2002, specifiek p. 58 e.v. en p. 679 e.v.
43 Nader bijv. 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.
44 Nader P. Hacker, 'Teaching fairness to artificial intelligence: existing and novel strategies against algorithmic discrimination under EU law', *Common Market Law Review* 2018, p. 1143-1186, op p. 1146 e.v.
45 Hierover o.m. Barocas & Selbst 2016 (noot 19); Hacker 2018 (noot 44).
46 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. 9-10.
47 Zie bijv. art. 137g Sr en 429quater Sr: beide bevatten een strafbaarstelling van discriminatie, maar in het laatstgenoemde artikel ontbreekt het opzetvereiste.

personen.[48] De toepasselijkheid van gelijkebehandelingsbepalingen, bijvoorbeeld in EU-richtlijnen of de Algemene wet gelijke behandeling, hangt echter af van de gronden waarop onderscheid wordt gemaakt (bijvoorbeeld geslacht).[49] Het gegeven dat vrijwel steeds sprake is van een pluraliteit aan gronden, leidt tot een kwalificatieprobleem voor wat betreft de toepasselijke wetgeving. Dit is van belang omdat specifieke gelijkebehandelingswetten vaak een hoger of een specifiek beschermingsniveau bieden als het gaat om directe discriminatie, bijvoorbeeld doordat een ongelijke behandeling op grond van geslacht alleen in een beperkt aantal omstandigheden is toegestaan. Is dan niet aantoonbaar dat een ongelijke behandeling primair of op doorslaggevende wijze is gebaseerd op geslacht, maar op tal van factoren, dan kan van deze bijzondere bescherming geen gebruik worden gemaakt.

Het concept van indirecte discriminatie biedt in de hiervoor omschreven gevallen soms uitkomst, maar is geen ideale oplossing. Zo kan indirecte discriminatie alleen worden vastgesteld als discriminerende effecten bij een groot aantal gevallen kunnen worden aangetoond, zodat een patroon van achterstelling op een bepaalde grond zichtbaar wordt gemaakt.[50] Ook hier doen zich bewijstechnische complicaties voor, in die zin dat een individu vaak niet zal weten of in andere gevallen ook sprake is van een ongelijke behandeling. Bovendien is het voor een individu niet altijd gemakkelijk om statistisch materiaal te verzamelen over het effect van een algoritme. Voor individuele slachtoffers van een ongelijke behandeling kan het daardoor moeilijk zijn om een succesvol beroep te doen op het discriminatieverbod.[51]

3.3 *Vrijheidsrechten*

3.3.1 *Grondrechtelijke kader*

Vrijheidsrechten zijn op velerlei plaatsen en manieren gecodificeerd, onder meer in de Grondwet, het EVRM en het Handvest. Het uitgangspunt daarbij is dat iedereen het recht heeft om zijn overtuigingen, gevoelens en meningen onder woorden te brengen en die te delen met anderen. Dat kan gebeuren in woord of geschrift, maar ook in de vorm van samenkomsten of protestacties of door het uitbrengen van een stem tijdens verkiezingen. De vrijheid van meningsuiting, vrijheid tot informatie, demonstratie- en verenigingsvrijheid en het kiesrecht zijn daarmee van essentieel belang in een democratische rechtsstaat.

Uit de uitwerking van deze rechten in de nationale en Europese rechtspraak blijkt, net als bij de privacyrechten, dat vrijheidsrechten niet absoluut zijn. Wel zijn er strikte eisen gesteld aan hun regulering. Zo kan de vrijheid van meningsuiting volgens artikel 7 Gw alleen door formele wetgeving worden beperkt als het gaat om schriftelijke uitingen en omvat deze bepaling een vergaand verbod op preventieve beperkingen ('verbod van voorafgaand verlof').[52] Inhoudelijke vereisten voor beperking zijn vooral te vinden in de rechtspraak van het EHRM. Daarbij heeft dit Hof steeds het grote belang van de vrijheidsrechten in een democratische samenleving vooropgesteld. 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 of zich te verenigen.[53]

De rechtspraak laat zien dat in de loop van de tijd ook een groot aantal verplichtingen voor de staat is aangenomen om deze vrijheidsrechten actief te beschermen; het gaat daarbij dus om zogenaamde positieve verplichtingen.[54] In dit verband kan in het bijzonder worden gewezen op de rechtspraak over informatiegaring, waarbij de overheid in een aantal gevallen actief informatie beschikbaar moet maken.[55] Meer algemeen moet de overheid ervoor zorgen dat mensen toegang hebben 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.[56] De staat moet daarbij 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.[57]
De vrijheidsrechten beschermen primair tegen handelen van de overheid. Toch heeft het EHRM bijvoorbeeld aangenomen dat van beheerders van webfora mag worden verwacht dat zij bepaalde uitingen weigeren als die haat zaaien of oproepen tot geweld.[58] Waar nodig kan dit voor de nationale rechter worden afgedwongen. Daardoor is tot op zekere hoogte sprake van 'horizontale werking', dat wil zeggen van werking van grondrechten in de relatie tussen burgers onderling.[59]

3.3.2 *Vrijheidsrechtelijke knelpunten*

Veel van de grondrechtelijke knelpunten die samenhangen met algoritmes houden verband met de positieve verplichtingen van de overheid om de uitoefening van vrijheidsrechten effectief te realiseren. Dit kan in het bijzonder aan de orde zijn als algoritmes worden ingezet door sociale

48 P. de Hert e.a., 'Big data en gelijke behandeling', in: P.H. Blok (red.), *Big data en het recht*, Den Haag: Sdu 2017, p. 125.
49 Daarnaast zijn deze bepalingen maar op een beperkt aantal terreinen van toepassing, zoals de arbeid; vgl. Hacker 2018 (noot 44), p. 1154 e.v.
50 Vgl. Hacker 2018 (noot 44), p. 1153.
51 Zie ook Hacker 2018 (noot 44), p. 1168.
52 A. Nieuwenhuis, 'Vrijheid van meningsuiting', in: J.H. Gerards e.a. (red.), *Grondrechten. De nationale, Europese en internationale dimensie*, Nijmegen: Ars Aequi Libri 2013, p. 96.
53 J.H. Gerards, 'Artikel 10. Vrijheid van meningsuiting', in: J.H. Gerards e.a. (red.), *Sdu Commentaar EVRM. Deel 1 – Materiële rechten* (online) 2017, C.4.1 en C.5.4.11.
54 Idem, C.3.2; Nieuwenhuis 2013 (noot 52), p. 87 e.v. Zie voor het concept positieve verplichtingen de bronnen vermeld in noot 30.
55 EHRM (GK) 8 november 2016, nr. 18030/11, ECLI:CE:ECHR:2016:1108JUD001803011 (*Magyar Helsinki Bizottság/Hongarije*), *EHRC* 2017/36, m.nt. T. McGonagle, par. 156.
56 EHRM 17 september 2009, nr. 13936/02 ECLI:CE:ECHR:2009:0917JUD001393602 (*Manole e.a./Moldavië*), par. 101-107.
57 Idem; zie Gerards 2017 (noot 53), C.3.2.
58 EHRM (GK) 16 juni 2015, nr. 64569/09 (*Delfi AS/Estland*), ECLI:CE:ECHR:2015:0616JUD006456909, *EHRC* 2015/172, m.nt. B. van der Sloot, *NJ* 2016/457, m.nt. E.J. Dommering, par. 54 e.v.
59 Zie voor nadere uitleg o.m. Gerards 2011 (noot 29), p. 263 e.v.

media en zoekmachines en daarbij leiden tot het ontstaan van 'filterbubbels'.[60] Deze bubbels kunnen de pluriformiteit en diversiteit van informatievoorziening raken, en kunnen daarmee impact hebben op de vrijheid om informatie te ontvangen. Dit zou kunnen leiden tot een positieve verplichting voor diezelfde overheid om het pluralisme van de media te beschermen en een goede toegang tot informatie te waarborgen.[61] Zo'n verplichting kan ook worden geformuleerd als het gaat om het bestrijden van het risico van 'chilling effects'. Het verlies van anonimiteit door grootschalige gegevensverzameling, -opslag en -analyse, kan tot gevolg hebben dat burgers hun meningen niet meer (op een bepaalde manier) durven over te brengen.[62] Dat geldt voor uitingen in de offline publieke ruimte, voor uitingen op sociale media en – door de opkomst van het IoT – voor uitingen in huiselijke sfeer.

Algoritmes kunnen verder worden ingezet ten behoeve van 'private censuur' door sociale media en zoekmachines.[63] Onwelgevallige, verdachte of gevaarlijke content kan worden herkend, waarna het bijvoorbeeld onmogelijk wordt om dit soort content te plaatsen of te downloaden, of waarna bepaalde content automatisch wordt verwijderd. Bijzondere grondrechtelijke knelpunten ontstaan als de staat inbreuk maakt op de vrijheid van meningsuiting door bedrijven te verplichten om bepaalde uitingen te verwijderen. Dan kan worden gesproken van indirecte publieke censuur.[64] De stelling kan zijn dat maatregelen noodzakelijk zijn ter bescherming van zwaarwegende belangen of andere grondrechten.[65] Zo kan het doel zijn om inbreuken op de eer en goede naam te voorkomen of om discriminatie tegen te gaan (bijvoorbeeld door haatzaaiende content direct te verwijderen).[66] Met dergelijke maatregelen moet echter uiterst zorgvuldig worden omgegaan. De bij het detecteren van problematische content gebruikte algoritmes kunnen fouten en *biases* bevatten. Bovendien bestaat het risico dat vooral controversiële, grove of kunstzinnige uitingen verwijderd zullen worden, omdat zij op de grens liggen tussen wat een algoritme als 'aanvaardbaar' of 'onaanvaardbaar' zal herkennen.[67] Met name voorafgaande beperkingen van uitingen door algoritmes verdienen bijzondere aandacht, omdat hierbij de mogelijkheid tot vrije meningsuiting vergaand wordt aangetast; door voorafgaande beperkingen kunnen uitingen immers al worden geblokkeerd nog voordat zij hun publiek bereiken. Artikel 7 Grondwet verbiedt dergelijke voorafgaande beperkingen van de vrijheid van meningsuiting volledig.

Andere knelpunten bij de vrijheidsrechten 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 discriminatie van bepaalde groepen. 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 bijvoorbeeld Big Data-analyse inzetten, hetgeen kan leiden tot inbreuken op privacy van individuele (aanstaande) leden of tot moeilijkheden bij het aanvechten van een mede op algoritmes gebaseerde beslissing om een vereniging te verbieden. Ook verenigingen zelf kunnen gebruikmaken van Big Data-analyses, bijvoorbeeld bij beslissingen over het toelaten of royeren van leden. Dergelijke beslissingen zijn, door hun potentiële ondoorzichtigheid, mogelijk lastig aan te vechten.

Tot slot kan de inzet van Big Data potentieel verstrekkende gevolgen hebben voor de uitoefening van het 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, Facebook en YouTube die bepalen welke informatie tot kiezers komt.[68] 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.[69] Op een vergelijkbare manier kunnen Big Data en het gebruik van algoritmes invloed hebben op de opkomst bij verkiezingen. Het passieve kiesrecht kan ten slotte worden geraakt als politieke partijen Big Data-analyses gebruiken bij het bepalen van de geschiktheid van potentiële kandidaten.

60 E. Pariser, *The Filter Bubble: How the New Personalized Web Is Changing What We Read and How We Think*, Londen: Penguin Books 2011 en F.J. Zuiderveen Borgesius e.a., 'Algoritmische verzuiling en filter bubbles: een bedreiging voor de democratie?', *Computerrecht* 2016/173 (p. 255-262).

61 Zie voor het concept positieve verplichtingen de bronnen vermeld in noot 30. Zie specifiek bijv. EHRM 17 september 2009, nr. 13936/02 ECLI:CE:ECHR:2009:0917JUD001393602 (*Manole e.a./Moldavië*), par. 101-107; EHRM 14 september 2010, nrs. 2668/07 e.a. (*Dink/Turkije*), *NJ* 2012/32, m.nt. E.J. Dommering, *EHRC* 2010/137, m.nt. R. van de Westelaken; zie ook Gerards 2017 (noot 53), C.3.2.

62 WRR 2016 (noot 6), p. 92 en 135.

63 K. Klonick, 'The New Governors: The People, Rules, and Processes Governing Online Speech', *Harvard Law Review* 2018, p. 1598-1670; Raso e.a. 2018 (noot 2) p. 38.

64 Vgl. 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; zie ook Raso e.a. 2018 (noot 2), p. 39.

65 Zie EHRM *Delfi AS* (noot 58).

66 Raso e.a. 2018 (noot 2), p. 38.

67 R. Tushnet, 'Power without responsibility: intermediaries and the First Amendment', *George Washington Law Review* 2008, p. 1015-1016; Raso e.a. 2018 (noot 2), p. 39.

68 Zie o.m. H. Hazenberg e.a., *Micro-Targeting and ICT media in the Dutch Parliamentary system. Technological changes in Dutch Democracy*, TU Delft, augustus 2018 (www.staatscommissieparlementairstelsel.nl/documenten/publicaties/2018/10/ 18/micro-targeting-and-ict-media-in-dutch-parliamentary-system_public); F.J. Zuiderveen Borgesius e.a., 'Online Political Microtargeting: Promises and Threats for Democracy', *Utrecht Law Review* 2018, p. 82-96.

69 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, p. E4512-E4521.

3.4 *Procedurele rechten*

3.4.1 *Grondrechtelijk kader*

Het recht op een eerlijk proces en het recht op een effectief rechtsmiddel, neergelegd in artikelen 6 en 13 EVRM en artikel 47 Hv, vertonen nauwe samenhang. In algemene zin blijkt uit de EHRM-rechtspraak over deze procedurele rechten dat een rechtsmiddel voldoende toegankelijk moet zijn, dat het rechtsmiddel een inhoudelijke beoordeling mogelijk moet maken en moet kunnen leiden tot effectief rechtsherstel,[70] en dat een rechterlijke uitspraak moet worden voorzien van een draagkrachtige motivering.[71] Daarnaast moet een rechter uiteraard onafhankelijk en onpartijdig zijn.[72] De procedurele waarborgen die moeten worden geboden zijn onder meer die van een eerlijke en open behandeling van een geschil. Bij dit laatste is vooral de gelijkheid van de procespartijen (*equality of arms*) van belang. Zo hebben beide partijen het recht om te worden gehoord en moeten zij effectief kunnen reageren op elkaars stellingen (hoor en wederhoor).[73] Ook moeten ze in gelijke mate in staat worden gesteld om relevant materiaal aan te dragen (zoals deskundigenberichten of documenten), moet worden voorzien in faire en evenwichtige regels omtrent bewijs, bewijslast en bewijslastverdeling, en moeten partijen in gelijke mate en voldoende in staat worden gesteld om het voor de zaak relevante materiaal te bestuderen en te betwisten.[74] Dit impliceert niet alleen openbaarheid en transparantie van de stukken, maar ook voldoende voorbereidingstijd voor de beide partijen om er effectief op te kunnen reageren.[75]

3.4.2 *Procedureelrechtelijke knelpunten*

Als algoritmes ten grondslag liggen aan beslissingen die de levens van mensen beïnvloeden, en dergelijke beslissingen in rechte worden aangevochten, kan dit invloed hebben op de uitoefening van het recht op een eerlijk proces en op toegang tot een effectief rechtsmiddel.[76] Tegelijkertijd kunnen algoritmes de rechter ondersteunen bij zijn oordeelsvorming of in de toekomst de rechter zelfs (gedeeltelijk) kunnen vervangen. Rondom deze twee constateringen doen zich enkele specifieke 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.[77] Zo kan algoritmische profilering leiden tot het opstellen van profielen die verbonden zijn met verdachte gronden als ras of seksuele gerichtheid.[78] Wanneer dergelijke profielen 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. Dit speelt in sterke mate bij slimme algoritmes, waarvan de exacte werking veelal niet direct duidelijk is. Komt een dergelijke zaak voor een rechter, dan kan de technologische en contextuele complexiteit van algoritme-gedreven besluitvorming er bovendien toe 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 een 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*, zoals in de rechtspraak van de Afdeling Bestuursrechtspraak van de Raad van State en de Hoge Raad al is onderkend.[79] Daarnaast kan de ondoorzichtigheid van algoritmes leiden tot een toenemende rol van IT-deskundigen in de rechtszaal. Procespartijen zullen niet altijd over gelijke (financiële) middelen beschikken om deze deskundigen op te roepen. Als dit onvoldoende wordt gecompenseerd, kan ook hierdoor sprake zijn van een ongelijke procespositie.

Als Big Data en KI worden ingezet ter ondersteuning van rechterlijke oordeelsvorming, kan dit rechters helpen om tot een kwalitatief goed oordeel te komen.[80] Er kunnen echter ook knelpunten optreden als het gaat om het recht op een onafhankelijke en onpartijdige rechter.[81] 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, die het bijvoorbeeld moeilijk maakt om te bepalen op welke inhoudelijke gronden hoger beroep kan worden ingesteld. In het verlengde hiervan 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.

70 M. Reiertsen, *The European Convention on Human Rights Article 13. Past, Present and Future* (diss. University of Oslo 2017), p. 213 e.v. en p. 248-250 e.v.

71 Zie o.m. T. de Jong, *Procedurele waarborgen in materiële EVRM-rechten* (diss. Leiden 2017), p. 33.

72 P.P.T. Bovend'Eert, *Rechterlijke organisatie, rechters en rechtspraak*, Deventer: Kluwer 2013, hoofdstukken 2 en 3.

73 De Jong 2017 (noot 71), p. 30.

74 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, p. 362.

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

76 Zie ook Raso e.a. 2018 (noot 2), p. 20 e.v.

77 M. Hildebrandt, *Smart Technologies and the End(s) of Law. Novel Entanglements of Law and Technology*, Cheltenham: Edward Elgar Publishing 2015, p. 101.

78 Raso e.a. 2018 (noot 2), p. 20.

79 ABRvS 17 mei 2017, ECLI:NL:RVS:2017:1259 (*AERIUS I*), ABRvS 18 juli 2018, ECLI:NL:RVS:2018:2454 (*AERIUS II*) en HR 17 augustus 2018, ECLI:NL:HR:2018:1316, r.o. 2.3.3.

80 H. Prakken, 'Komt de robotrechter er aan?', *NJB* 2018/207 (p. 269-274).

81 J.E.J. Prins & J. van der Roest, 'AI en de rechtspraak: Meer dan alleen de 'robotrechter'', *NJB* 2018/206 (p. 260-268).

4. Grondrechtelijke knelpunten in samenhang bezien

Paragraaf 3 heeft laten zien dat de beschikbaarheid van algoritme-gedreven technologieën kan leiden tot een breed palet aan grondrechtelijke knelpunten. Dit vindt zijn oorzaak primair in de 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 deze technologieën 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 deze laatste paragraaf besproken.

4.1 *Actoren en rechtsverhoudingen*

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 leiden tot inbreuken op de privacyrechten. Als de overheid algoritmes inzet in het veiligheidsdomein of deze gebruikt bij differentiatie 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 technologiegedreven infrastructuur, leidt tot 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 veel grondrechtelijke aandacht 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 kunnen 'kleinere' private actoren als verenigingen, politieke partijen en kleine bedrijven gebruikmaken van algoritme-gedreven besluitvorming. De hiervoor omschreven surveillanceproblematiek strekt zich bijvoorbeeld uit tot werkgevers die het gedrag van hun werknemers monitoren, terwijl gelijkebehandelingsproblemen zich kunnen voordoen in de relatie tussen aanbieders en afnemers van diensten. Een dergelijke invloed van algoritme-gedreven technologieën in uiteenlopende 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. Anders gezegd: de knelpunten kunnen zich zowel doen in verticale rechtsverhoudingen (d.w.z. tussen de staat en private actoren) als in horizontale verhoudingen (d.w.z. tussen private actoren onderling). Vanuit het perspectief van de grondrechtencodificaties is het echter wel degelijk van belang onderscheid te blijven maken tussen horizontale en verticale rechtsverhoudingen. Grondrechtelijke knelpunten moeten op verschillende manieren geadresseerd worden, afhankelijk van de vraag door wie een inbreuk wordt veroorzaakt. Daarbij is van belang dat het in de huidige juridische constellatie nog 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 een bedrijf in een civiele procedure wordt verplicht om grondrechten te respecteren. Welk optreden van overheidsactoren of private spelers precies nodig is, is moeilijk in zijn algemeenheid te zeggen; dit zal steeds afhangen van de verantwoordelijke actor, de aard van de betrokken belangen en de manier waarop een algoritme inbreuk maakt op een grondrecht.

4.2 *Urgentie van de grondrechtelijke knelpunten*

De in paragraaf 3 geïdentificeerde knelpunten laten een grote samenhang zien tussen de verschillende grondrechtenclusters. 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 algoritme-gedreven besluitvorming, en waar prioriteiten moeten worden gesteld bij het optreden tegen door algoritmes veroorzaakte grondrechteninbreuken. Hoogstens kunnen sommige van de benoemde knelpunten vanuit grondrechtelijk oogpunt worden beschouwd als minder urgent. In de afwezigheid van hard empirisch bewijs van bijvoorbeeld 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. 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 menselijke, niet-neutrale, complexe en ondoorzichtige 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 tot 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 een transparante en kenbare motivering van (publiekrechtelijke en privaatrechtelijke) beslissingen die zijn gebaseerd op of mede zijn ingegeven door 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 temeer problematisch nu knelpunten bij de uitoefening van procedurele rechten raken aan de effectiviteit van andere 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 voldoet aan de eisen van het recht op een eerlijk proces. 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 grondrechten, maar komt ook adequate rechtsbescherming tegen dergelijke schendingen onder druk te staan. Om deze redenen verdienen ook de knelpunten bij de uitoefening van procedurele rechten urgente aandacht.