Waardig digitaal overheidsbestuur

Over een integere omgang met sensor-technologie, big data, algoritmen en het Internet of Things

waag
technology & society

Maaike Kamps
Waag, Amsterdam
November 2018

Dankwoord

Waag en provincie Noord-Holland hebben mij in de gelegenheid gesteld dit essay te schrijven via een 'Open Government Fellowship' bij Waag. Voor zowel Waag als mij was het fellowship een nieuwe ervaring. Wat mij betreft heeft het geleid tot een vruchtbare uitwisseling van kennis en ervaringen. Ik ben Waag en haar medewerkers dankbaar voor hun tijd, interesse en kritische blik.

Daarnaast hebben enkele anderen mij geholpen bij het ontwikkelen en aanscherpen van mijn visie op ethiek in relatie tot het gebruik van nieuwe technologieën. Mijn dank gaat dan ook uit naar Mona de Boer, Douwe Schmidt, Willem Koeman, Paul Strijp, Mira Heesakkers, Pim van der Pol, Carin Kamps en Feiko Vrieze.

Dit essay is op persoonlijke titel geschreven.

Haarlem, 2018
Maaike Kamps

decode

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 732546.

decodeproject.eu

Inhoudsopgave

Dankwoord **2**

Management samenvatting **4**
(Deel)oplossingen 5
Borging 5

1. Inleiding **7**
De Vierde industriële Revolutie 7
Maatschappelijke druk om kansen te benutten 7
Mogelijke negatieve gevolgen 8
Doel, vraagstelling en afbakening 8
Leeswijzer 9

2. Borging van publieke waarden in rechten en beginselen **10**
Publieke waarden 10
» Grondrechten 10
» Algemene beginselen van behoorlijke bestuur 10
Code goed openbaar bestuur 11
Het Tada-manifest 12
Concluderend 13

3. Het vergaren en gebruiken van gegevens **14**
Big data 14
Privacy-knelpunten bij datavergaring 15
Sensortechnologie 17
Internet of Things 18
Concluderend 18

4. Het openbaren en delen van gegevens **20**
Het beginsel van transparantie 20
De keerzijde van transparantie 21
» Function creep 21
» Profilering 22
Dataminimalisatie 22
Concluderend 23

5. Het verwerken van gegevens via algoritmen **25**
De tekortkomingen van algoritmen 26
Bescherming tegen uitwassen 27
Onuitlegbare en oncontroleerbare algoritmen 27
Een afweging met betrekking tot algoritmen 28
Het algoritme impact assessment 29
Concluderend 29

6. Conclusies en aanbevelingen **31**
Publieke waarden in het geding 31
Borging in de organisatie 32

Overzicht van gebruikte bronnen **34**

Management samenvatting

Dit essay belicht vier samenhangende technologische ontwikkelingen waar overheden in toenemende mate gebruik van maken, te weten big data, sensortechnologie, algoritmen en het Internet of Things. Centraal hierin staat het vergaren, openbaren, delen, verwerken en gebruiken van data.

Het is aantrekkelijk voor overheden om deze nieuwe technologieën te gebruiken, want ze maken het mogelijk om overheidstaken efficienter en effectiever uit te voeren, wat een van de beginselen is van 'goed openbaar bestuur'. Hierbij komen wel enkele publieke waarden in het gedrang.

Om welke publieke waarden gaat het dan? Bij gebruik van sensortechnologie gaat het om privacy en transparantie. Er worden 'in het algemeen belang' data over burgers verzameld zonder dat deze burgers altijd weten waar en wanneer dit gebeurt en met welk doel, en zonder dat burgers daarvoor toestemming hebben gegeven. Daarbij hebben burgers vaak geen inzicht in en invloed op wat er vervolgens met die gegevens gebeurt. Deels komt dit omdat overheden zich – wellicht uit onervarenheid -- onvoldoende houden aan de Algemene Verordening Gegevensbescherming (AVG). Maar ook als overheden zich wél aan de AVG houden, zijn niet alle knelpunten opgelost. Als burgers toestemming wordt gevraagd voor datavergaring, is het mede door de stapeling van initiatieven voor burgers ondoenlijk om steeds te achterhalen en te doorzien waarvoor ze eigenlijk toestemming geven. Het wordt bovendien steeds moeilijker voor de burger om zich aan datavergaring in de openbare ruimte te onttrekken. De keuzevrijheid van de burger die onbespied wil blijven om te gaan en staan waar hij wil, wordt hiermee ingeperkt. En als informatie over de burger vervolgens gebruikt wordt ten behoeve van gedragssturing, kan dezelfde burger zich ook nog eens gemanipuleerd voelen.

Bij het Internet of Things speelt iets soortgelijks zich af. Als het gaat om interactie van overheidsapparatuur met apparaten die burgers gebruiken, verplaatsen vraagstukken met betrekking tot transparantie, privacy, toestemming, keuzevrijheid en gedragssturing zich deels naar de privésfeer omdat apparaten veelal daar gebruikt worden. Voor wat betreft gedragssturing is er wel een ethische standaard ontwikkeld waaraan dit zou moeten voldoen, maar toepassing hiervan moet dan wel geborgd zijn in de overheidsorganisatie die aan gedragssturing doet. Het is de vraag of dit momenteel voldoende gebeurt.

De AVG heeft als doel de privacy te beschermen, maar de AVG is niet 'waterdicht'. Bovendien krijgen niet-persoonlijke data steeds vaker karakteristieken van persoonlijke data. Het daarom van belang dat transparant is wanneer en hoe overheden persoonlijke én niet-persoonlijke data voor welk doel verzamelen, zodat de burger daar zélf kennis van kan nemen en bezwaar kan maken indien hij zich toch in zijn privacy aangetast voelt. Hier ligt een spanningsveld omdat we zien dat de Wet open overheid, die proactieve openbaring van gegevens afdwingt, stagneert.

Tegelijkertijd zit er echter ook een keerzijde aan transparantie over data. Als inzichtelijk is over welke data overheden beschikken, kunnen deze data opgevraagd worden. Ten eerste kunnen persoonlijke data door andere overheden opgevraagd worden om ze binnen een nieuwe context te gebruiken. Deze vorm van *function creep* druist in tegen het zogeheten 'doelbindingsprincipe' van de AVG, maar de AVG kent uitzonderingen hierop en het zal maar al te verleidelijk zijn voor overheden om hiervan gebruik te maken. Ten tweede kunnen private partijen data opvragen. De overheid zal deze data vervolgens met deze partijen moeten delen in het kader van de Wet hergebruik overheidsinformatie. Zoals gezegd zijn data te de-anonimiseren en krijgen niet-persoonlijke data steeds vaker persoonlijke kenmerken. Hier zit dus alsnog een privacy-risico.

Tot slot worden (big) data verwerkt met behulp van algoritmen. Ook dit is niet onomstreden. Zo kan het ontwerp van een algoritme leiden tot discriminerende effecten en zogenoemde 'feedback loops'. Daarnaast is er sprake van toenemende complexiteit van algoritmen, waardoor algoritmen straks niet meer uitlegbaar en/of controleerbaar zullen zijn en waardoor

openheid, transparantie en accountability in het gedrang komen. Als algoritmen niet openbaar zijn en gecontroleerd (kunnen) worden, blijven eventuele ongewenste bijwerkingen onzichtbaar.

(Deel)oplossingen

Hoe kunnen overheden dan de ongewenste bijwerkingen en effecten van de inzet van digitale technologieën voorkomen of verminderen? In dit essay zijn allerlei (deel)oplossingen aangedragen voor bovengenoemde problemen, zoals:

- Een sensordataregister, waardoor inzichtelijk wordt welke overheid welk type data in de openbare ruimte vergaart. Dit lost het probleem van verminderde keuzevrijheid echter nog niet op. Om te voorkomen dat hele gemeenten onbegaanbaar worden voor burgers die niet van monitoring gediend zijn, dient een zeer kritische afweging gemaakt te worden tussen algemeen belang en individueel belang. Deze afweging kan alleen door de volksvertegenwoordiging gemaakt worden.
- In situaties waarin het praktisch gezien ondoenlijk is om expliciet de toestemming van iedere burger te vragen voor datavergaring- of verwerking, of waar verwacht wordt dat burgers door de bomen het bos niet meer zullen zien, zou die toestemming in ieder geval bij de volksvertegenwoordiging opgehaald moeten worden.
- Er zijn maatstaven ontwikkeld voor gedragssturing, opdat dit niet uitmondt in manipulatie. Deze maatstaven moeten dan uiteraard wel gehanteerd worden. Hier is kaderstelling en controle voor nodig.
- De AVG is ingesteld om de privacy te beschermen. Helaas is de AVG niet 'waterdicht' en op termijn – als bijna alle data 'persoonlijke data' worden – onhoudbaar. Alleen vergaande dataminimalisatie en access control kunnen aantasting van de privacy helpen voorkomen. Hier zijn technische hulpmiddelen voor in ontwikkeling.
- Het ontwikkelen van 'technologisch burgerschap' zou burgers weerbaar maken tegen de invloeden van digitalisering. Hier mogen we echter niet te veel van verwachten. Ten eerste vereist zo'n ontwikkeling een denk- en doenvermogen dat veel mensen ontberen, ten tweede zullen juist de zelflerende algoritmen straks ook voor experts niet goed meer te volgen zijn. Niettemin is het belangrijk dat de burgers die er wél enigszins toe in staan zijn, de kans krijgen zich hierin te ontwikkelen en de kar kunnen trekken voor hen die dat niet kunnen. Gemeenteraden en Provinciale Staten moeten dan wel het algemeen belang bewaken.
- Tot slot is een toezichtscommissie of 'waakhond' genoemd voor controle op ingewikkelde algoritmen en hun effecten. Zo'n kennisbundeling van expertise lijkt me nuttig en nodig, maar dit vereist dan wel eerst een afweging binnen overheidsorganisaties in welke beleidsvelden welk type algoritmen ingezet mogen worden. Zo'n afweging is een politieke keuze, en het is daarom van belang deze afweging bij raadsleden en statenleden te leggen.

De consequentie van dataminimalisatie en het niet gebruiken van oncontroleerbare algoritmen, is wel dat er soms maatschappelijke kansen onbenut zullen blijven. Het is aan gemeenteraden en Provinciale Staten om over deze gemiste kansen verantwoording af te leggen aan de burger.

Borging

Het is dus mijns inziens vooral aan overheden zelf om meer sturing en richting te geven aan een integere omgang met nieuwe technologieën. Dit betekent dat politici, bestuurders en ambtenaren de benodigde technologisch, juridische en ethische kennis in huis moeten hebben of aan moeten weten te boren. Juist zij zullen zich moeten ontwikkelen tot 'technologisch burger'.

Het begint natuurlijk bij besef van de problematiek. Een lokaal en regionaal debat om de publieke waarden in relatie tot digitalisering te doorleven, lijkt me dan ook zinvol. Het Amsterdamse manifest Tada kan een aanzet geven tot zo'n debat, maar zou niet domweg 'overgenomen' moeten worden. Het is juist van belang dat alle betrokkenen gezamenlijk tot eigen conclusies komen.

In de meeste ambtelijke overheidsorganisaties is nu nog niet voldoende technologische en

ethische kennis aanwezig om goed vorm te geven aan een integere omgang met de digitalisering van overheidstaken. In beleidsafdelingen zal een zekere basiskennis van de materie nodig zijn, juist om te weten wanneer men hulp moet inroepen van specialisten. Dit zal in interne opleidingstrajecten geborgd moeten worden.

Wat betreft interne specialistische ondersteuning, is het belangrijk te beseffen dat de vereiste deskundigheid vaak niet aanwezig zal zijn bij de ICT-afdelingen en dat het onlogisch is dit extern in te huren. Het is dan handig om de eventueel al aanwezige kennis van data, ethiek en dergelijke zoveel mogelijk te bundelen en indien nodig aan te vullen met extra deskundigheid.

Verder is het natuurlijk van belang dat overheden hun ethische principes ook als uitgangspunt nemen ingeval de private sector betrokken wordt bij de taakuitvoering van de overheid. Hierbij is het een nationale 'digitaliseringsakkoord' zinvol om de private sector bewust te maken van het feit dat de overheid wellicht extra zware eisen stelt aan te leveren producten en diensten. Deze dialoog wordt naar verwachting concreter – en daarmee zinvoller - als er overeenstemming is tussen overheden over wat die eisen dan zouden moeten zijn.

1. Inleiding

De Vierde industriële Revolutie

Sinds pakweg tien à vijftien jaar komt er een aantal ontwikkelingen bij elkaar die gecombineerd zorgen voor een enorme technische en maatschappelijke versnelling, die wel geduid wordt als 'de Vierde Industriële Revolutie'. Het gaat dan om technologische, biomedische en sociale ontwikkelingen op het gebied van internet en sociale media, sensortechnologie, Big data, algoritmen, blockchain, 'het internet der dingen', virtual reality, biotechnologie, nanotechnologie en 3D-printing. Deze genoemde technologieën zijn overigens lang niet altijd nieuw, want sommigen waren al bekend in de jaren '50 van de vorige eeuw. Wat nieuw is, is de toegenomen rekenkracht van computers en de beschikbaarheid van grote hoeveelheden data, evenals de wijze waarop de genoemde technologieën samenkomen en elkaar versterken en versnellen, en zich verweven tot nieuwe productietechnieken, producten en businessmodellen. Men kan daardoor sneller, efficiënter en goedkoper organiseren en produceren. En dat kan weer leiden tot meer maatwerk, minder ruimtegebruik voor productie en opslag, hogere productiviteit en kostenbeheersing, minder en ander grondstoffengebruik, en minder brandstofgebruik.

Dit essay belicht vier technologische ontwikkelingen uit deze Vierde Industriële Revolutie die momenteel sterk in de belangstelling van overheden staan. Het gaat dan om big data, sensortechnologie, algoritmen en Internet of Things. De samenhang tussen deze technologieën is als volgt: overheden verzamelen steeds grotere hoeveelheden gegevens ofwel 'big data', mede met gebruikmaking van sensortechnologie. Big data worden via algoritmen verwerkt en kunnen zo een bron worden voor innovaties die het leven gemakkelijker en aangenamer maken. Datadeling en algoritmen maken het mogelijk dat apparaten met elkaar communiceren zonder tussenkomst van de mens. Dit wordt het 'Internet of Things' (IoT) genoemd. Centraal in deze ontwikkelingen staat het vergaren, openbaren, delen, verwerken en gebruiken van data. De maatschappelijke druk om deze technologieën in te zetten is groot, maar er zitten keerzijden aan het gebruik van deze technologieën. Dit essay focust zich op de vraag hoe overheden hier integer mee om kunnen gaan.

Maatschappelijke druk om kansen te benutten

Het samenspel van sensortechnologie, big data, algoritmen en IoT biedt grote kansen voor de maatschappij op het gebied van welvaart en welzijn. Voor (lagere) overheden en hun uitvoeringsdiensten kun je concreet denken aan meer efficiëntie en effectiviteit bij hun taakuitvoering, bijvoorbeeld op het gebied van toezicht en handhaving (*predictive policing*): als je bijvoorbeeld weet waar criminaliteit meer voorkomt, kun je aldaar maatregelen nemen of meer handhaven. Ook wat verkeersveiligheid betreft liggen er kansen: 95% van de ongelukken in het verkeer komt door menselijk handelen, terwijl met rijtaakondersteuning de veiligheid kan verbeteren (Rijkswaterstaat, z.d.). Wat betreft verkeer en vervoer is bovendien de verwachting dat de behoefte aan mobiliteit en transport in de Randstad tot 2040 met 20% tot 46% gaat groeien, afhankelijk van het economisch scenario (NMCA, 2017, p. 45). Als de informatiesystemen van (autonome) auto's onderling én met de infrastructuur gegevens uitwisselen, kan dat de verkeersdoorstroming ten goede komen en kunnen auto's dichter op elkaar rijden. Hierdoor kan de bestaande infrastructuur waarschijnlijk een deel van de verwachte volumegroei opvangen. Gegevensuitwisseling maakt ook 'Mobility as a Service' mogelijk, een Spotify-achtige dienst waarbij de consument mobiliteit van deur tot deur via een willekeurige combinatie van vervoermiddelen inkoopt, wat reistijden kan verkorten. Op zeven plekken in het land wordt hiermee al geëxperimenteerd (Rijksoverheid, 2018). Verder kan digitalisering de transitie naar duurzame energie en een circulaire economie versnellen. Het is bijvoorbeeld maar de vraag of de energietransitie op tijd gaat slagen als de balancering van het elektriciteitsnet via elektrische auto's (een vorm van Internet of Things) niet tot stand komt.

Al deze kansen op grotere efficiëntie en effectiviteit in ogenschouw genomen, is het niet verwonderlijk dat overheden druk aan het experimenteren zijn met nieuwe technolo-

gieën, vaak met gebruikmaking van Europese subsidies (Naafs, 2017). Zowel op het gebied van mobiliteit als duurzame energie biedt het Europese Horizon 2020-programma de nodige financiële ondersteuning voor 'smart oplossingen' (Europese Commissie, 2014). Daarbij komt dat Nederlandse overheden, Noord-Holland in bijzonder, de potentie hebben om voorop te lopen: de MRA is hét dataknooppunt (*datahub*) van Europa aan het worden. Door aanwezigheid van de Amsterdam Internet Exchange (AMS-IX) en de vele datacenters zijn zowel de digitale infrastructuur en fysieke datacapaciteit aanwezig, en daarmee het vermogen om hierop innovatieve data-gedreven toepassingen te bouwen, voor zowel bedrijfsleven en overheden als burgerinitiatieven.

Een andere reden om nieuwe digitale technologieën in te zetten is de verwachte productiviteitsstijging. Hierbij moet opgemerkt worden dat volgens de economische wet van Baumol de productiviteit bij de overheid door inzet van nieuwe technologieën naar verwachting wel zal toenemen, maar dat deze zal achterblijven bij de private sector. Bij de arbeidsintensieve dienstensector - waar de publieke sector deel van uitmaakt - is productiviteitsgroei door nieuwe technologie immers moeilijker te bewerkstelligen dan bij de technologiegedreven industriële sector. Dit zal de overheid gaandeweg relatief duur maken ten opzichte van de private sector. Misschien kan de maatschappij die kosten best dragen, maar de vraag is natuurlijk of daar de politieke wil voor zal zijn. Daarbij speelt een en ander zich af in een context van vergrijzing en krimp van de beroepsbevolking.

Al deze ontwikkelingen zullen naar verwachting leiden tot maatschappelijke druk op de overheid om de kansen die er liggen, te benutten en overheidstaken niet alleen goedkoper en effectiever, maar ook met minder menskracht uit te voeren. Er zit echter wel een keerzijde aan de digitalisering van overheidstaken.

Mogelijke negatieve gevolgen

Zoals de eerste Industriële Revolutie enerzijds welvaart bracht, en anderzijds leidde tot kinderarbeid, uitbuiting en stedelijke overbevolking, zo kent ook de Vierde Industriële Revolutie een aantal mogelijke negatieve gevolgen. Denk aan verlies aan privacy, verlies aan democratische controle, discriminatie, sociale uitsluiting en vervreemding. Juist door deze aspecten te onderzoeken, te erkennen en erop in te grijpen, kunnen we grote misstanden veelal nog vóór zijn. Gaandeweg komt hier meer aandacht voor, niet alleen in Nederland, maar wereldwijd. In India woedt bijvoorbeeld een debat over privacy bij het gebruik van de grootste biometrische overheidsdatabank ter wereld (Safi, 2018). In de VS klinkt de roep om een digitale 'bill of rights' (Issa, 2012). En in Brazilië zijn de privacyrechten van burgers in 2014 in wetgeving vastgelegd (Framework, 2018).

De toegenomen aandacht voor de negatieve kanten van digitalisering heeft ook in Europa geresulteerd in regelgeving, zoals de Europese Algemene Verordening Gegevensbescherming (AVG). Kamervragen hebben in Nederland geleid tot onderzoek naar het gebruik van big data en algoritmen door de overheid (Kamerbrief, 2018). En in Amsterdam is een publiek debat gevoerd over publieke waarden in relatie tot de digitale samenleving. Dit heeft geleid tot het manifest 'Tada, duidelijk over data', dat inmiddels een plaats heeft gekregen in het coalitieakkoord van het Amsterdams gemeentebestuur (Coalitieakkoord, 2018). De vraag is echter of regelgeving als de AVG en een manifest als Tada voldoende houvast bieden aan overheden om op integere wijze om te gaan met data en de technologieën die daarbij een rol spelen.

Doel, vraagstelling en afbakening

Met dit essay hoop ik bij te dragen aan het debat en de visievorming omtrent een integere toepassing van nieuwe technologieën door overheden, door inzicht te geven in ethische dilemma's en mogelijke oplossingen. De focus ligt vooral op de lagere overheden, vanwege mijn persoonlijke achtergrond bij provincie en gemeenten. De centrale kwestie is hoe (lagere) overheden de kansen kunnen benutten die sensortechnologie, big data, algoritmen en Internet of Things bieden, zonder de publieke waarden waarop onze democratische rechtsstaat gestoeld is, geweld aan te doen. Dit leidt eerst tot de vraag welke waarden in het geding zijn.

Daarna welke dilemma's zich voordoen in relatie tot die waarden, en wat overheden kunnen of zouden moeten doen om integer te handelen. Tot slot komt de vraag aan de orde wat een integere omgang met nieuwe technologieën betekent voor de manier waarop de overheden zouden moeten gaan werken en georganiseerd zijn.

In dit essay wordt niet ingegaan op de bemiddelende, regelstellende en handhavende rol die de overheid heeft of kan hebben bij de toepassing van nieuwe technologieën door de private sector. Deze rol is mijns inziens veelal (maar niet altijd) voorbehouden aan Rijk en vooral de EU, vanuit oogpunt van gelijk speelveld. Dat laat onverlet dat lagere overheden een signalerende en agenderende rol kunnen hebben om ethische knelpunten bij digitalisering in de publieke en private sector op rijksniveau aan de orde te stellen, zeker gezien het feit dat de netwerkende overheid steeds vaker haar taken vervult in samenwerking met niet-overheden.

In dit essay wordt verder meestal over 'burgers' gesproken, en niet over 'inwoners'. Dit is een bewuste keuze, die benadrukt dat de rechtsverhouding tussen het individu en de overheid centraal staat.

Leeswijzer

Dit essay is als volgt opgebouwd. In het eerste hoofdstuk komen de publieke waarden aan de orde die in het geding zijn bij genoemde technologieën. Daarbij wordt bekeken in hoeverre een Amsterdams voorbeeld -- het zogenoemde 'Tada-manifest' – nieuwe inzichten biedt. De hoofdstukken daarna focussen op de dilemma's die aan de orde zijn bij sensortechnologie, Internet of Things, big data en algoritmen, mede in relatie tot de eerder genoemde publieke waarden. Hierbij wordt in hoofdstuk 3 vooral ingegaan op het vergaren en gebruiken van big data, in hoofdstuk 4 op het openbaren en delen van data, en in hoofdstuk 5 op het verwerken van data door middel van algoritmen. Dit resulteert in een aantal aanbevelingen in hoofdstuk 6.

2. Borging van publieke waarden in rechten en beginselen

In dit hoofdstuk komen publieke waarden aan de orde die in het geding zijn bij de inzet van de in het vorige hoofdstuk genoemde technologieën. Deze waarden komen tot uitdrukking in wet- en regelgeving. Daarna wordt ingegaan op de vraag hoe een manifest als Tada, dat probeert 'nieuwe' regels of beginselen te definiëren voor een digitale samenleving, zich verhoudt tot de bestaande wet- en regelgeving. Biedt Tada ons nieuwe inzichten?

Publieke waarden

Pim van der Pol, integriteitscoördinator bij Provincie Noord-Holland, omschrijft ethiek als 'welke waarden je tot uitgangspunt neemt' en integriteit als 'dat je volgens de waarden handelt' (persoonlijke communicatie, 9-4-2018). Wat betekent dat voor de overheid? We kennen als maatschappij een aantal publieke waarden die leidraad zijn voor het overheidshandelen:

- dat mensen gelijkwaardig zijn;
- dat het individu beschermd moet worden tegen te grote machtsuitoefening door de overheid;
- dat in een democratische rechtstaat burgers hun overheid moeten kunnen controleren;
- dat in een vrijemarkteconomie burgers collectief eigenaar zijn van de middelen die een overheid verzamelt of genereert en dat de overheid sober en doelmatig met deze middelen om moet gaan.

Deze waarden komen tot uitdrukking in wet- en regelgeving. Ten eerste liggen de grondrechten van de burger verankerd in hoofdstuk 1 van de grondwet (GW) en in het Europees Verdrag voor de Rechten van de Mens (EVRM). Ten tweede kennen we in Nederland de tien 'algemene beginselen van behoorlijk bestuur' (abbb), die in jurisprudentie zijn ontwikkeld en deels zijn gecodificeerd in de Algemene wet bestuursrecht. Daarnaast moet beleid en beleidsvorming voldoen aan de Code goed openbaar bestuur.

Grondrechten

De grondrechten geven burgers persoonlijke vrijheid en bescherming tegen te grote machtsuitoefening door de overheid. In een digitale of digitaliserende samenleving zijn er twee van groot belang: het recht op privacy (GW art. 10; EVRM art. 8), dat in het geding is bij het verzamelen en verwerken van gegevens, en het recht op gelijke behandeling en het verbod op discriminatie (GW. art 1; EVRM art. 14) dat in het geding is bij het toepassen van algoritmen, zoals in hoofdstuk 5 aan de orde zal komen. De Europese Algemene Verordening Gegevensverwerking (AVG) die afgelopen jaar van kracht is geworden, bekrachtigt het recht op informationele privacy door duidelijk te maken wat wel en niet mag bij het verzamelen en verwerken van gegevens.

Algemene beginselen van behoorlijke bestuur

De abbb zijn van toepassing op bestuurlijke besluiten. Binnen de context van digitalisering van overheidstaken zijn de volgende van belang:

- Het motiveringsbeginsel (art. 3:46 Awb) vereist dat een overheid haar besluiten goed moet motiveren: de feiten moeten kloppen en de motivering moet logisch en begrijpelijk zijn: waarom is het besluit genomen, op welke gronden en welke afwegingen zijn gemaakt? Dit vereist ten eerste transparantie over welke gegevens worden gebruikt om tot besluitvorming te komen en ten tweede uitleg hoe deze gegevens dan zijn verzameld en verder zijn verwerkt, ook als die verwerking met behulp van algoritmen is gedaan.
- Het zorgvuldigheidsbeginsel (art. 3:2 Awb) vereist dat een bestuur een besluit zorgvuldig moet voorbereiden én nemen. Dit vereist onder meer het gebruik van correcte, actuele gegevens en het gebruik van volledige informatie, dus álle relevante gegevens. Dat kan trouwens ook een advies van een deskundige zijn, of het horen van belanghebbenden. Je zou in dit kader ook kunnen stellen dat als een algoritme ten grondslag ligt aan een besluit, dit algoritme getoetst zou moeten zijn op objectiviteit en dat eventuele bijwerkingen bekend moeten zijn.
- Het evenredigheidsbeginsel vereist dat de

overheid ervoor moet zorgen dat de lasten of nadelige gevolgen van een overheidsbesluit voor een burger niet zwaarder zijn dan het algemeen belang van het besluit (art. 3:4 lid 2 Awb). Dit is wellicht van belang in de opkomende zogenoemde 'slimme' wijken, waarin gemeenten volop experimenteren met het waarnemen, analyseren en sturen van het gedrag van burgers: is deze handelwijze wel te rechtvaardigen onder verwijzing naar het algemeen belang?

- Volgens het rechtszekerheidsbeginsel moet de overheid haar besluiten zó formuleren dat de burger precies weet waar hij aan toe is of wat de overheid van hem verlangt. Bovendien moet de overheid de geldende rechtsregels juist en consequent toepassen. Burgers moeten er zeker van zijn dat hun recht wordt gedaan en burgers moeten bezwaar in kunnen dienen als zij menen dat zij onrechtvaardig of onrechtmatig behandeld worden. Een onrechtvaardige of onrechtmatige behandeling kan aan de orde zijn bij gebruik van algoritmen bij beleids- en besluitvorming, maar om bezwaar in te kunnen dienen moet de burger wel weten dat algoritmen een rol spelen en welke rol dat dan is.

Code goed openbaar bestuur

De kwaliteit van het openbaar bestuur wordt vaak uitgedrukt met de term 'good governance'. Governance gaat over de wijze waarop een overheid bestuurt en gezag uitoefent. Het gaat daarbij om de instituten, de wet- en regelgeving, de processen (o.a. de samenwerking met publieke en private stakeholders) en de institutionele middelen die ingezet worden. Om de governance te beoordelen, zijn maatstaven ontwikkeld. In Nederland heeft het ministerie van Binnenlandse Zaken in 2009 de 'Code goed openbaar bestuur' gedefinieerd, zodat alle overheidsinstanties volgens dezelfde richtlijnen (kunnen) handelen (Ministerie van Binnenlandse Zaken, 2009). De Code bevat zeven beginselen over de verhouding tussen overheden en hun burgers en de wijze waarop overheden om dienen te gaan met publieke middelen, te weten:

1. Openheid en integriteit.
   Dit gaat onder meer over de mate waarin beleidsinformatie toegankelijk en begrijpelijk is voor de burger. Beleid dat is gebaseerd op zeer ingewikkelde algoritmen of onbekende data, zal niet snel voldoen aan dit beginsel.
2. Participatie.
   Dit gaat over de mate waarin burgers in de gelegenheid worden gesteld om hun ideeën en meningen in te brengen, wat het draagvlak voor beleid kan vergroten en beleid democratisch kan legitimeren. Worden burgers wel voldoende betrokken bij keuzes omtrent digitalisering van de overheidstaakuitvoering?
3. Behoorlijke contacten met burgers.
   Dit gaat enerzijds over bereikbaarheid van de overheid, anderzijds over duidelijkheid met betrekking tot wat de burger van de overheid mag verwachten. De Raad van State waarschuwt in dit kader dat de minder zelfredzame burger kans loopt de weg kwijt te raken tussen alle digitale mogelijkheden en regels (Raad van State, 2018).
4. Doelgerichtheid en doelmatigheid.
   Het overheidsbestuur maakt de doelen bekend en zet de beschikbare publieke middelen daarbij zo efficiënt mogelijk in. Het gaat dus om het bereiken van het doel met gebruik van zo min mogelijk middelen. Dit is relevant, want de maatschappelijke verwachting is dat het werken met sensortechnologie, big data, algoritmen en Internet of Things tot meer efficiëntie en effectiviteit in de taakuitvoering zal leiden.
5. Legitimiteit: het overheidsbestuur oefent haar gezag uit in overeenstemming met geldende wet- en regelgeving. De beslissingen zijn te rechtvaardigen.
6. Lerend en zelfreinigend vermogen.
   Het overheidsbestuur is zodanig ingericht dat ze haar eigen handelen voortdurend evalueert en op basis van de uitkomsten haar handelen verbetert. Ze leert daarbij van andere overheden en laat zich controleren. Dit is uiteraard van belang nu veel overheden worstelen met een correcte omgang met alle nieuw beschikbare technische mogelijkheden.
7. Verantwoording (accountability).
   Dit gaat over de mate van bereidheid van het overheidsbestuur om zich jegens de omgeving te verantwoorden. Dit zal naar verwachting lastig worden als steeds ingewikkeldere algoritmen ten grondslag liggen aan beleids- en besluitvorming. De vraag

hierbij is hoe ver een overheid moet of kan gaan met zich verantwoorden.

Het Tada-manifest

Zoals hierboven uiteengezet, roepen de abbb en de Code goed openbaar bestuur vragen op in relatie tot de digitalisering van de overheidstaken. Hetzelfde soort vragen heeft in Amsterdam geleid tot een debat over publieke waarden in relatie tot de digitale samenleving. Dit heeft geresulteerd in het manifest 'Tada, duidelijk over data' (Tada, 2017). Het manifest heeft een aantal nieuwe regels of beginselen geformuleerd:

1. Inclusiviteit: iedereen doet mee, iedereen participeert.
2. Zeggenschap: burgers houden zeggenschap over hun persoonlijke data
3. De menselijke maat: deze blijft leidend
4. Openheid en transparantie
5. Gelegitimeerd en gecontroleerd: democratisch totstand gekomen en beoordeeld.
6. Eigenaarschap: data zijn van iedereen, voor iedereen

Als we dan kijken hoe deze Tada-beginselen zich verhouden tot de beginselen die we al kennen, vallen enkele zaken op. Ten eerste wordt 'inclusiviteit' in de Code van het ministerie niet expliciet genoemd, maar 'participatie' wel. Er zit veel overlap tussen deze begrippen. Inclusiviteit houdt in dat de overheid een proces of project zodanig inricht dat iedereen mee kan doen en niemand wordt uitgesloten van deelname. Het doel van inclusiviteit is brede participatie, wat kan leiden tot beleidsverrijking, draagvlak voor beleidskeuzes en democratische legitimatie van overheidsbesluiten.

Het tweede Tada-beginsel van 'zeggenschap' is geborgd in artikel 6 en 7 van de AVG, waarin staat dat er sprake moet zijn van expliciete toestemming van een betrokkene voordat zijn gegevens verwerkt kunnen worden. En het derde beginsel, 'de menselijke maat blijft leidend', zien we impliciet terug in de abbb, die erop gericht zijn de individuele burger te beschermen tegen de macht van de overheid.

Het menselijke maat-beginsel van Tada gaat volgens Willem Koeman, een van de betrokkenen bij het formuleren van Tada, echter ook over de omgang met de toenemende complexiteit van algoritmen en het beleid en de besluiten die daarop gebaseerd zijn (persoonlijke communicatie, 21-9-2018): deze beleids- en besluitvorming moet nog wel te bevatten zijn voor mensen.

Wat betreft het vierde beginsel van Tada ('openheid en transparantie'), dit komt geheel overeen met het eerste beginsel van de Code. De eis van 'transparantie' vinden we overigens ook terug in artikel 5 van de AVG, waarin gesteld wordt dat persoonsgegevens 'moeten worden verwerkt op een wijze die ten aanzien van de betrokkene rechtmatig, behoorlijk en transparant is' en in artikel 12 dat vereist dat een betrokkene op de hoogte moet worden gesteld van het feit dat er verwerking van zijn persoonsgegevens plaatsvindt, en wat de doelen van deze verwerking zijn.

Het vijfde Tada-beginsel ('gelegitimeerd en gecontroleerd') komt deels overeen met de legitimiteitseis van de Code goed openbaar bestuur. Het beginsel van democratische controle is echter minder specifiek uitgewerkt in de abbb of de Code. De in de Code genoemde 'participatie' is immers niet hetzelfde als 'democratische controle'.

Het laatste Tada-beginsel ('iedereen is eigenaar van data') lijkt op het eerste gezicht op gespannen voet te staan met het tweede beginsel van Tada ('zeggenschap van de individuele burger over zijn persoonlijke gegevens'). Het gaat bij het beginsel van gezamenlijk eigenaarschap echter om niet-persoonlijke danwel geanonimiseerde data en bij het beginsel van zeggenschap om persoonlijke data. Zoals in navolgende hoofstukken duidelijk zal worden, is 'individuele zeggenschap' geborgd in de nieuwe AVG die vereist dat toestemming aan burgers wordt gevraagd om hun gegevens te verzamelen en te verwerken. Het beginsel van gezamenlijk eigenaarschap is geborgd in Nederlandse wetgeving, en wel in de Wet hergebruik overheidsinformatie. In navolgende hoofdstukken zal echter duidelijk worden dat er toch een spanningsveld tussen de beginselen van persoonlijke zeggenschap en gezamenlijk eigenaarschap blijft bestaan, omdat in de toekomst de grens tussen persoonlijke en niet-persoonlijke data zal vervagen.

Al met al blijkt dat het Tada-manifest in grote mate overlap vertoont met bestaande burgerrechten en beginselen. Dat is niet vreemd, omdat ze allen gestoeld zijn op dezelfde publieke waarden: dat het individu tegen te grote machtsuitoefening door de overheid beschermd moet worden, dat in een democratische rechtstaat burgers hun overheid moeten kunnen controleren, en dat in een vrijemarkteconomie burgers collectief eigenaar zijn van hetgeen een overheid verzamelt of genereert.

Concluderend

In dit hoofdstuk is een aantal publieke waarden onder de loep genomen die een belangrijke rol spelen bij het digitaal verzamelen, openbaren, delen en verwerken van gegevens. Deze waarden komen tot uitdrukking in wet- en regelgeving. Er blijkt veel overlap te zijn tussen bestaande wet- en regelgeving en het Amsterdamse Tada-manifest. De waarde van Tada ligt mijns inziens dan ook niet zozeer in het manifest als resultaat, maar in het proces ernaartoe. Het gaat erom dat de publieke waarden doorleefd worden en betekenis krijgen voor betrokkenen, nu er een nieuwe context is ontstaan door de digitalisering van overheidsbestuur. En soms is daar een pakkende herformulering bij nodig.

In de navolgende hoofdstukken worden de dilemma's die spelen bij sensortechnologie, big data, algoritmen en Internet of Things in beeld gebracht. In hoeverre botsen de deze technologische ontwikkelingen met publieke waarden en wat kan er gedaan worden om ze in overeenstemming te brengen?

3. Het vergaren en gebruiken van gegevens

Het vergaren van data heeft een grote vlucht genomen. Waar het om persoonsgegevens gaat, zorgt de Algemene Verordening Gegevensbescherming voor bescherming van de privacy. Daarmee zijn echter niet alle knelpunten op het gebied van privacy opgelost. Ook spelen er kwesties op het gebied van transparantie, toestemming en keuzevrijheid.

Big data

Het verzamelen van gegevens ten behoeve van de commercie, de wetenschap of overheidsbeleid is natuurlijk niet nieuw. De overheid verzamelt en gebruikt van oudsher allerlei soorten data ten behoeve van haar taakuitvoering. De provincie Noord-Holland onderscheidt bijvoorbeeld bestuurlijke data, die direct ten grondslag liggen aan besluiten van het provinciaal bestuur, en overige data die ondersteunend zijn aan de uitvoering van overheidstaken. Dat kunnen gegevens zijn over mensen, over objecten, of over de leefomgeving (PNH, 2017). Wél nieuw is dat het verzamelen van gegevens in een stroomversnelling is gekomen. Het gaat dan steeds vaker om 'big data'.

Wanneer zijn gegevens 'big data'? Adviesbureau Gartner neemt kort en bondig een aantal 'V's als uitgangspunt (Gartner, z.d.). Big data kenmerken zich door hun Volume, Verscheidenheid en 'Velociteit' ofwel snelheid. Hoogleraar Frans Feldberg voegt hier 'portabiliteit' (overdraagbaarheid) en 'interconnectiviteit' (uitwisselbaarheid en daarmee integratie van data) aan toe (Feldberg, 2018). Ook de potentiële invloed van big data wordt met de letter 'V' geduid: door interessante toepassingen kunnen big data waarde ofwel 'Value' genereren. Kortom, gegevens worden 'big data' als het gaat het om constante stromen van gegevens uit allerlei bronnen, die al dan niet gecombineerd leiden tot enorme gegevensverzamelingen die continu worden ververst, geanalyseerd en uitgebreid en waarmee waarde kan worden gecreëerd.

Als data persoonsgegevens bevatten, is sinds 25 mei 2018 de Algemene Verordening Gegevensbescherming (AVG) van kracht. De AVG versterkt de privacy-rechten van Europese burgers, en legt meer verantwoordelijkheid voor bescherming van die privacy-rechten bij data-verzamelende en –verwerkende organisaties, op straffe van fikse boetes. In de AVG is helder vastgelegd wat wel en niet mag bij het verzamelen en verwerken van persoonlijke data, ook als daarbij samengewerkt wordt met andere partijen.

Belangrijke waarborgen voor de privacy zijn te vinden in artikel 25 van de AVG. Dit artikel gaat in op 'gegevensbescherming door ontwerp en door standaardinstellingen'. Privacy-door-ontwerp (*privacy by design*) houdt in dat een ICT-toepassing dusdanig ontworpen moet zijn dat de privacy zo goed mogelijk gediend is. Een voorbeeld hiervan is data-minimalisatie: dat houdt in dat je niet meer gegevens opvraagt dan dat je nodig hebt om je taak uit te voeren. Als iemand bijvoorbeeld alcohol koopt, hoeft de verkoper slechts te weten of iemand 18 is of niet, en zijn andere persoonlijke gegevens als geslacht, woonplaats en geboortedatum irrelevant. Ook hoeven die gegevens niet eeuwig te worden bewaard en hoeft niet iedereen ze te kunnen inzien (*acces control*). Gegevensbescherming door standaardinstellingen (*privacy by default*) houdt in dat de standaardinstellingen (*default options*) voorzien in zo groot mogelijk privacy, en de gebruiker zelf in actie moet komen als hij gegevens van zichzelf alsnog wil openbaren.

Handhaving van de door de AVG opgelegde regels vindt plaats door middel van boetes, die opgelegd worden door de toezichthouder. In Nederland is dat de Autoriteit Persoonsgegevens. Een aantal overtredingen valt onder een hoog boeteregime. Dit zijn meestal duidelijk meetbare overtredingen: er is toestemming gevraagd om data uit te wisselen of niet; er is inzage in data gegeven of niet; gegevens zijn gewist of niet. Vereisten als privacy-door-ontwerp en access control vallen echter onder een lager boeteregime, omdat deze niet als 'fundamentele verplichting' van de verwerkingsverantwoordelijke wordt beschouwd. Het lastige aan deze vereisten is dat ze minder eenduidig meetbaar zijn. Wanneer vinden we een ontwerp goed en wanneer matig? Ook kunnen er bij-

voorbeeld verschillende uitkomsten zijn op de vraag wie er gegevens moeten kunnen inzien, afhankelijk van hoe een proces of organisatie georganiseerd is. Hierdoor is juridisch ingewikkelder om te beoordelen in welke mate een organisatie aan de AVG voldoet.

Al met al komt het er bij privacy-door-ontwerp en access control vooral op neer of gemaakte keuzes goed verantwoord kunnen worden. Om dit door gemeenteraden en Provinciale Staten te kunnen laten controleren is het van belang dat politici voldoende kennis hebben van alternatieve mogelijkheden voor zo'n ontwerp.

Privacy-knelpunten bij datavergaring

Het is verder van belang te beseffen dat de AVG niet alle huidige en toekomstige privacy-knelpunten oplost. Een eerste knelpunt betreft de reikwijdte van de AVG. De AVG gaat over persoonsgegevens en definieert dit in artikel 4 als 'alle informatie waaraan een natuurlijk persoon direct of indirect kan worden geïdentificeerd' (AVG, p. 33). Denk hierbij aan NAW-gegevens, maar het kan ook gaan om een online identificator, of om elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van een persoon. Hier vallen dus data over iemands gedrag niet onder. Desondanks kunnen burgers zich in hun privacy aangetast voelen als gegevens verzameld worden over hun gedrag om bijvoorbeeld de verkeersdoorstroming te bevorderen of om het elektriciteitsnet te balanceren.

De Tilburgse wetenschapper Nadezhda Purtova wijst er bovendien op dat de technologische ontwikkelingen zo snel gaan, dat bijna ieder niet-persoonlijk gegeven straks herleidbaar zal zijn tot een individu en daarmee een persoonsgegeven wordt (Purtova, 2018). Een voorbeeld hiervan is een IP-adres van een computer, dat via data bij een service provider altijd wel weer tot een specifiek persoon herleidbaar is. En Amerikaanse wetenschappers hebben inmiddels aangetoond dat je met vier vage informatiepunten (vier aankopen via een willekeurige credit card op vier locaties) het merendeel van de kopers kon identificeren (Hardesty, 2015).

Het verst hierbij gaat het internationale burgercollectief Bellingcat, dat een veelheid aan aanwijzingen combineert om te bepalen wie wanneer waar aanwezig was om zo identiteiten van daders en slachtoffers bloot te leggen. Bellingcat-lid Christiaan Triebert, die Turkse coupplegers wist te identificeren, zei daarover tegen de NOS: "Met enige training kan iedereen dit doen. Het is geen magie, het is heel veel zoeken. Ik heb alleen openbare informatie gebruikt". En: "We gebruiken bijvoorbeeld tweets, geotags, foto's, filmpjes en die checken we met elkaar om informatie te verifiëren. We zoeken niet naar één naald in één hooiberg, maar naar duizenden naalden in duizenden hooibergen" (NOS-bericht, 2016). De vraag is dan hoe lang de huidige AVG houdbaar zal zijn. Als alle data in potentie persoonlijke data is, wordt de AVG straks naar verwachting, in de woorden van Purtova,"*a law of everything, well-meant but impossible to maintain*" (Purtova, 2018).

Als iedere individu identificeerbaar is door het combineren van de juiste datasets, wordt ook het onderscheid dat de AVG maakt in 'gepseudonimiseerde' en 'geanonimiseerde' data irrelevant. De AVG is in principe alleen van toepassing op zogenoemde 'gepseudonimiseerde data' en niet op geanonimiseerde gegevens, ervan uitgaande dat geanonimiseerde gegevens niet meer terug te herleiden zijn tot individuele personen. In de praktijk gaat dit dus niet op. Tom Demeyer, CTO bij onderzoeksinstituut Waag zegt hierover: "Totaal anonimiseren bestaat eigenlijk niet. Al is het maar omdat je niet weet welke datasets er in de toekomst beschikbaar komen waarvan je met behulp door de methodiek van correlatie-analyse alsnog persoonlijke gegevens uit geaggregeerde gegevens terug kunt halen" (persoonlijke communicatie, 31-8-2018).

Een bijkomend privacy-aspect dat de AVG niet oplost is de afhankelijkheid van buitenlandse technologiebedrijven die datasets verzamelen, maar waar we onvoldoende controle over hebben. Hoogleraar Aiko Pras wijst er in *De Groene Amsterdammer* op dat vaak Amerikaanse servers worden gebruikt en dat deze onder Amerikaanse wetgeving vallen, zodat de Amerikaanse overheid toegang tot die servers kan opeisen.[1] Andere delen van de digitale infrastructuur zijn volgens hem in Chinese handen (Naafs, 2017).

Je kunt je afvragen of (delen van) de digitale infrastructuur niet onder de hoede van Europese nutsbedrijven zouden moeten vallen, als we de privacy in Europa daadwerkelijk willen waarborgen. De Europese Commissie heeft hier inmiddels aandacht voor, zo blijkt uit het Next Generation Internet Initiative dat onderzoekt hoe Europese waarden binnen een nieuw internet geborgd zouden kunnen worden (Europese Commissie 2018).

Al me al kunnen we hieruit concluderen dat als niet-persoonlijke data steeds gemakkelijker (terug) te herleiden zijn tot persoonlijke data, het van belang is om ook het verzamelen van niet-persoonlijke data te minimaliseren. Want data die er niet zijn, kunnen ook niet misbruikt worden. Voorafgaand aan de keuze om data te verzamelen, zouden dan vragen gesteld moeten worden als: In hoeverre dragen de gezochte data de potentie in zich om in de toekomst persoonlijke data te worden? Is het nodig om al deze data te verzamelen om deze overheidstaak uit te voeren? Kan het ook anders of met minder?

Momenteel wordt er gewerkt aan een specifieke vorm van dataminimalisatie. Dit gaat om digitale identificatiemethoden op basis van zogenoemde 'attributen', ofwel brokjes informatie die wat zeggen over de persoon in kwestie. De burger die zich op enigerlei wijze moet identificeren, kan vervolgens iedere keer alleen dat attribuut vrijgeven dat nodig is voor de betreffende dienst of product. In Nijmegen wordt hier al mee geëxperimenteerd en de gemeente legt goed uit hoe het werkt: "IRMA haalt brokjes informatie op uit officiële registratiesystemen van instanties, waardoor de gebruiker via IRMA alleen noodzakelijke gegevens kan verstrekken. Met de app kan iemand bijvoorbeeld laten zien dat hij ouder is dan 18 zonder dat de geboortedatum en andere persoonsinformatie zichtbaar zijn." (Gemeente Nijmegen, 2018). Socrates Schouten, medewerker bij Waag, merkt overigens hierover op dat dit weer heel nieuwe vragen oproept, zoals wie deze infrastructuur dan beheert en welke businessmodellen hier achter zitten (persoonlijke communicatie, 1-11-2018). Hier is politieke kaderstelling en controle bij nodig.

1 De VS worden onder de AVG als 'veilig' land gezien. Wel moet voldaan worden aan het zogeheten 'Privacy Shield'. Dit is een regeling tussen de VS en de EU waarbij de VS aangeeft de Europese regels na te zullen leven. 'Nationale veiligheid' is echter wel een grond voor toegang voor de Amerikaanse overheid.

Sensortechnologie

Een van de manieren waarop de overheid big data verzamelt, is via de inzet van sensortechnologie in de openbare ruimte. Sensoren (waaronder camera's) worden steeds kleiner en goedkoper en daardoor beter toepasbaar. Uit onderzoek van Platform voor Onderzoeksjournalistiek Investico is dan ook gebleken dat aardig wat steden aan het experimenteren zijn geslagen met sensortechnologie. Ze houden zich daarbij echter vaak niet aan de bestaande privacywetgeving (Naafs, 2017).[2] Zo moeten burgers eigenlijk vooraf worden geïnformeerd over het feit dat data over hen worden verzameld en met welk doel. Dat gebeurt niet of onvoldoende (Naafs, 2017). Er wordt in deze gevallen ook geen toestemming aan burgers gevraagd. Dit probleem speelt nog steeds, ook nu de AVG van kracht is. In Enschede heeft een inwoner onlangs de Autoriteit Persoonsgegevens gevraagd om handhavend tegen de gemeente op te treden in verband met wifi-tracking waar hij geen toestemming voor geeft (Borghuis, 2018). Filosoof Helen Nissenbaum maakt er bovendien op attent dat ingeval er wel om toestemming wordt gevraagd, het burgers lang niet altijd duidelijk zal zijn waarvoor ze toestemming geven, mede omdat het ondoenlijk is dat telkens te achterhalen (Berinato, 2018). De stapeling van initiatieven in de openbare ruimte versterkt dit nog eens.

Het Rathenau Instituut ziet nog een bijkomend vraagstuk, namelijk die van de 'ethiek van het living lab' (Van Est et al, 2018, pp. 59-77). Waar vroeger experimenten in laboratoria plaatsvonden, vinden ze nu soms plaats in de publieke ruimte, zoals in de wijk Stratumseind in Eindhoven (Van Est et al, 2018, p. 89). Ook de provincie Noord-Holland ziet zichzelf als proeftuin voor 'slimme voertuigen' die kunnen communiceren met verkeerslichten en wegkantsystemen (Provincie Noord-Holland, 2018a). En bij de Praktijkproef Amsterdam laten weggebruikers zich via een app verspreiden over het wegennet (Praktijkproef Amsterdam, 2017). Burgers worden daarmee al dan niet onwetende proefkonijnen.

Dit brengt ons op het punt van de keuzevrijheid. Er is nu nog sprake van enkele locaties waarop geëxperimenteerd wordt, maar wat als dit straks in een hele gemeente gebeurt? In hoeverre kunnen burgers er straks nog voor kiezen om niet gemonitord te worden of als proefkonijn te fungeren, als dat betekent dat een groot deel van de gemeente onbegaanbaar voor hen wordt? En als de vergaarde data over de burger vervolgens gebruikt wordt ten behoeve van gedragssturing, in hoeverre wordt dezelfde burger dan gemanipuleerd?

Het Rathenau Instituut wijst de overheid op haar verantwoordelijkheden bij digitalisering. Enerzijds is de overheid verantwoordelijk voor het ontwikkelen en uitvoeren van beleid omtrent het gebruik van sensoren in de openbare ruimte, anderzijds voor de data die deze sensoren genereren (Est, 2018, pp. 99-100). Het Rathenau Instituut wil daarom dat er regels komen, en stelt bovendien voor een 'ethische toetsingscommissie voor onderzoek in de publieke ruimte' op te richten (Est, 2018, p. 107). Zo'n toetsingscommissie heeft echter wel kaders nodig om aan te toetsen. Deze kaderstelling valt onder de verantwoordelijkheid van de politiek. De belangenafweging die een digitaal experiment in de openbare ruimte vereist, is immers typisch iets wat in de politieke arena thuishoort. Hetzelfde geldt voor het stellen van voorwaarden aan zo'n experiment. De volksvertegenwoordiging zal de nut en noodzaak van dataverzameling in de openbare ruimte kritisch moeten beoordelen om te voorkomen dat onder het mom van 'algemeen belang' de burger overal en altijd gemonitord wordt. Zeker in een situatie waarin het praktisch gezien ondoenlijk is expliciet de toestemming van iedere burger te vragen, zou die toestemming in ieder geval bij de volksvertegenwoordiging opgehaald moeten worden.

Stichting Geonovum heeft alvast een concept-hulpmiddel opgesteld, de *Handreiking Spelregels Data Ingewonnen in de Openbare Ruimte* (Geonovum, 2017). In deze concept-handreiking worden niet alleen aanbevelingen gedaan voor de overheden zelf, maar ook voor de wijze waarop ze samenwerken met andere overheden en private partijen. Belangrijk element van de concept-handreiking is een model voor een gemeentelijke sensordata verordening, die onderdeel zou kunnen

2 Het onderzoek van Investico betreft 2017. Toen was de Wet bescherming persoonsgegevens (Wpb) nog van kracht, en niet de Algemene Verordening Gegevensbescherming. Onder de Wpb was echter ook al toestemming van betrokkenen vereist.

zijn van de APV. Hierin worden kwesties als meldingsplicht en vergunningsplicht geregeld. Centraal staat echter een zogeheten 'sensordataregister', waarin op metaniveau per gemeente bijgehouden kan worden waar welke data wordt verzameld met welk doel. Proeven die rijk of provincies doen op het gemeentelijk gebied, zouden dan ook bij het gemeentelijke register aangemeld moeten worden.

Dit waardevolle initiatief van Geonovum maakt kaderstelling voor en democratische controle op digitale projecten én hun cumulatieve effecten mogelijk. Tegelijkertijd zou zo'n register echter aan private partijen inzichtelijk maken waar interessante data te vinden zijn, die de overheid vervolgens zal moeten delen in het kader van de Wet hergebruik overheidsinformatie. De dilemma's die dit oplevert, komen in het volgende hoofdstuk aan de orde.

Internet of Things

Bovengenoemde vraagstukken beperken zich niet tot de openbare ruimte, maar strekken zich via het Internet of Things (IoT) uit tot in de privésfeer. Bij het IoT communiceren apparaten met elkaar zonder tussenkomst van de mens. Hiertoe vergaren apparaten data en delen ze deze data onderling, vervolgens worden de data verwerkt met behulp van algoritmen. Veel van die apparaten staan straks bij burgers in huis.

Ook bij het IoT dringt de vraag zich op in hoeverre transparant is wat er met gegevens gebeurt, in hoeverre de burger nog privacy geniet en in welke mate de burger nog de keuzevrijheid heeft om zich aan het IoT te onttrekken: biedt de netbeheerder straks nog wel analoge elektriciteitsmeters aan, of alleen nog maar 'slimme' meters? Is er straks nog een auto te koop die níet communiceert met de weginfrastructuur? En welke gegevens geven deze apparaten dan aan wie of wat door? Daarnaast spelen nog andere ethische kwesties een rol bij het IoT: wie is er verantwoordelijk voor de keuzes die door een apparaat worden gemaakt? In hoeverre kan een eigenaar de zelfstandige acties van zijn apparaat overrulen of ongedaan maken? En leidt gebrek aan controle over apparatuur op den duur niet tot een gevoel van vervreemding?

Vaak zal uit de gegevens die apparaten genereren het gedrag van de gebruiker kunnen worden afgeleid. Deze informatie leent zich voor gedragssturing. Om de burger hierbij te beschermen tegen manipulatie, zou gedragssturing volgens wetenschappers Thaler en Sunstein aan drie voorwaarden moeten voldoen, namelijk die van transparantie, keuzevrijheid en eigenbelang (Thaler en Sunstein, 2008). Transparantie houdt in dat bekend moet zijn wie de gedragssturing toepast, met welk doel en via welke gedragswijziging. Bij keuzevrijheid moet een burger een reële keuze hebben tussen zijn 'oude' gedrag en het gewenste nieuwe gedrag. Een bepaalde keuze mag dus geen 'straf' opleveren in de vorm van extra kosten of sancties. Ten derde moeten er goede redenen zijn voor burgers om te denken dat het gedrag dat aangemoedigd wordt, in hun eigen belang is.

De voorwaarden die (Nobelprijswinnaar) Thaler en Sunstein geformuleerd hebben, zijn inmiddels een gouden standaard geworden voor het beoordelen van gedragssturing vanuit een ethisch perspectief. Het gebruik van die standaard dient echter wel geborgd te zijn in een overheidsorganisatie. Zo zou de overheid die aan gedragssturing doet, verantwoording aan de burger moeten afleggen over zowel het gekozen doel als de methodiek. Daarnaast zou de keuze voor het toepassen van gedragssturing expliciet aan de volksvertegenwoordiging moeten worden voorgelegd, omdat hier sprake is van een afweging tussen maatschappelijke en individuele belangen. Het is de vraag of dit momenteel voldoende gebeurt.

Concluderend

Steeds vaker houden overheden zich bezig met big data. De AVG biedt daarbij duidelijkheid over wat persoonlijke data zijn en hoe deze vergaard en verwerkt mogen worden. Een knelpunt is echter de trend dat niet-persoonlijke data steeds vaker herleidbaar zijn tot individuen, en dat dus eigenlijk alle data op termijn onder de AVG zouden gaan vallen. De AVG wordt dan praktisch onhoudbaar. Hier is nog geen oplossing voor voorzien, anders dan het prudent omgaan met het verzamelen van niet-persoonlijke data.

Een ander knelpunt is dat als het verzamelen

van data in de openbare ruimte is toegestaan in het algemeen belang, dit kan betekenen dat burgers zich voortdurend bekeken voelen en delen van de openbare ruimte moeten gaan mijden om zich aan die monitoring te onttrekken. Als burgers al toestemming wordt gevraagd voor datavergaring, is het mede door de stapeling van initiatieven voor diezelfde burgers ondoenlijk om steeds te achterhalen en te doorzien waarvoor ze eigenlijk toestemming geven. Het wordt nog ingewikkelder bij het Internet of Things, omdat dit zich kan uitstrekken tot het privédomein van burgers. Gemeenteraden en Provinciale Staten zouden vanuit hun kaderstellende rol nut en noodzaak van deze vorm van datavergaring zeer kritisch moeten beoordelen. Zij zouden zich bewust moeten zijn van de dilemma's en deze vorm van datavergaring slechts op een beperkt aantal locaties moeten toestaan, gekoppeld aan een duidelijk doel. Ook zouden ze moeten bepalen wanneer gedragssturing wel of niet wenselijk is en controleren of gedragssturing voldoet aan de voorwaarden die Thaler en Sunstein geformuleerd hebben.

4. Het openbaren en delen van gegevens

In het voorafgaande hoofdstuk is onder meer ingegaan op ethische knelpunten bij datavergaring en -verwerking. In dit hoofdstuk wordt ingegaan op dilemma's bij het openbaren en delen van data. Hoe hiermee om te gaan?

Het beginsel van transparantie

In een democratische rechtstaat moeten burgers het overheidshandelen kunnen controleren. Nu uit het vorige hoofdstuk is gebleken dat de AVG de privacy niet geheel weet te beschermen, is het des te belangrijker dat transparant is wanneer en hoe overheden persoonlijke én niet-persoonlijke data voor welk doel verzamelen, zodat de burger daar kennis van kan nemen en bezwaar kan maken indien hij zich in zijn privacy aangetast voelt. Ook kan dan gecontroleerd worden of de gegevens rechtmatig verkregen zijn, of ze accuraat en betrouwbaar zijn, en of ze geschikt zijn voor het doel waarvoor ze verzameld zijn. Hoe is dan met die transparantie gesteld?

We kennen in Nederland de Wet openbaarheid van bestuur (Wob, 1991). Onder deze wet is overheidsinformatie in principe openbaar, al zijn er uitzonderingen, bijvoorbeeld ter bescherming van de privacy. Informatie wordt op verzoek beschikbaar gesteld, wat betekent dat diegene die informatie opvraagt zich ervan bewust moet zijn dat de overheid over de betreffende informatie beschikt.

Momenteel is er een opvolger van de Wob in de maak, de Wet open overheid (Woo). Die moet leiden tot snellere en meer proactieve openbaring[3] in plaats van openbaring op verzoek. Indien de Wet open overheid er komt, zijn bovendien niet alleen publieke, maar ook semi-publieke overheidsinstellingen (bijvoorbeeld musea en bibliotheken) verplicht proactief te laten zien over welke documenten/gegevens de organisatie beschikt. Bijvoorbeeld via een register. Daarnaast moeten bestuursorganen uitgebreider dan bij de Wob motiveren waarom ze openbaarmaking weigeren.

Er is de nodige kritiek op de Wet open overheid, namelijk dat Woo onuitvoerbaar zou zijn, dat ze haar doel voorbij schiet en dat er andere, goedkopere opties zijn. Uit quickscans in opdracht van de Tweede Kamer blijkt dat de invoering van de wet onevenredig veel geld en tijd zou gaan kosten, en dat de Provinciewet en Gemeentewet zouden moeten worden aangepast om geheimhouding van bepaalde besluiten te waarborgen (Kuipers, Van der Steenhoven & Staal 2016; 2017). De Raad van State zet dan ook haar vraagtekens bij de Woo (Raad van State, 2012). Politicus Harry van Zon wijst erop dat met een Woo weliswaar een berg aan informatiedragers beschikbaar komt, maar dat burgers vervolgens met een 'sisyfusklus' [sic] worden opgezadeld om hun weg te zoeken binnen de informatieoverload die dat oplevert. Een goede index op onderwerp is voor de burger volgens hem veel interessanter dan een register van wat er is (Van Zon, 2018). Andere critici zien meer in een betere omgang met de Wob, door instelling van een onafhankelijk orgaan dat Wob-verzoeken snel en vakkundig beoordeelt, zonder bemoeienis van de overheid waarbij het Wob-verzoek is ingediend (Elibol, 2018). Het is dan ook geen wonder dat de Wet open overheid momenteel stagneert in de Eerste Kamer. Niettemin heeft de gemeente Amsterdam het Tada-manifest met het principe 'eigenaarschap: data zijn van iedereen, voor iedereen' als uitgangspunt genomen. Dit roept verwachtingen op met betrekking tot meer proactieve openbaring van gegevens. Zoals in deze paragraaf geschetst, zal dat geen sinecure zijn.

Als maatschappij vinden we niet alleen het openbaren, maar ook het delen van gegevens belangrijk. Dit komt voort uit de gedachte dat alle burgers mede-eigenaar zijn van de middelen die een overheid verzamelt ten behoeve van haar taakuitvoering. Bovendien kan het openbaren en delen van overheidsinformatie bijdragen aan waardecreatie, in de vorm van innovatieve producten en diensten. Een voorbeeld van waardecreatie is Buienradar, een toepassing die door een private partij is gebouwd op basis van gegevens die verzameld worden door onder meer overheidsinstantie KNMI.

3 Met 'openbaren' wordt dan bedoeld: in een format dat toegankelijk en leesbaar is met de gebruikelijke computersoftware; waarbij er geen toestemming nodig is van eigenaar en waarbij de informatie gratis of tegen kostprijs beschikbaar is.

De gedachte van collectief eigenaarschap in combinatie met de wens tot waardecreatie heeft geleid tot de Wet hergebruik overheidsinformatie (Who, 2015). Deze wet legt de verplichting voor de overheid vast om overheidsinformatie op verzoek (niet proactief dus) beschikbaar te stellen in een herbruikbaar format, bepaalde uitzonderingen daargelaten. De Who is in principe ook van toepassing op geanonimiseerde persoonsgegevens.

De Who is in aanvulling gekomen op de eerder genoemde Wob en zorgt voor een duidelijker onderscheid in het doel van openbaarmaking van gegevens: democratische controle (Wob) versus economische waardecreatie (Who). De Wet open overheid zou grotere openbaarheid afdwingen dan de huidige wetgeving, en daarmee kunnen leiden tot meer hergebruik van gegevens.

De keerzijde van transparantie

Het openbaren en delen van data kent ook zijn keerzijde. Als inzichtelijk is over welke data overheden beschikken, kunnen deze data opgevraagd worden. Ten eerste kunnen persoonlijke data door andere overheden opgevraagd worden om ze binnen een nieuwe context te gebruiken (*function creep*). Ten tweede kunnen bedrijven data opvragen waarvan we in het vorige hoofdstuk hebben gezien dat deze data wellicht weer terug te herleiden zijn tot persoonlijke gegevens.

Function creep

Function creep betreft het benutten van gegevens voor geheel andere doeleinden dan waarvoor de gegevens oorspronkelijk verzameld zijn, zonder toestemming van de betrokken burgers. Bij function creep kan het gaan om het delen van gegevens binnen de eigen organisatie, met andere overheden of het opvragen van gegevens bij private partijen. Function creep schendt niet alleen de privacy, maar ook het recht op digitale soevereiniteit, door internetpionier Marleen Stikker omschreven als het recht om zelf te besluiten 'in welke relatie je wat van jezelf prijsgeeft' (Meijer & Schouten, 2017).

Function creep druist in tegen het zogeheten 'doelbindingsprincipe' van de AVG (artikel 5). Doelbinding wil zeggen dat persoonlijke gegevens alleen verzameld mogen worden voor een specifiek en goed omschreven doel. De AVG maakt function creep echter niet onmogelijk, want er zijn uitzonderingsgronden. Het gaat dan bijvoorbeeld om kwesties in het kader van de volksgezondheid, het verstrekken van een uitkering of medische zorg, rechtsvordering en strafrecht, wetenschappelijk onderzoek of een publieke taak in het algemeen belang, welke dan ook nog eens een grondslag dient te hebben in nationale wetgeving. Deze uitzonderingsgronden bieden overheden nog behoorlijk wat ruimte voor function creep. Ruimte die ongetwijfeld benut en misschien wel opgerekt zal worden. In een wat oudere, maar niet minder relevante publicatie van het Wetenschappelijk Onderzoek en Documentatiecentrum (WODC) wordt namelijk uitgelegd waarom overheden per definitie geneigd zijn tot function creep:

> De neiging om een maatregel bedoeld als oplossing voor een bepaald probleem ook toe te passen op een ander probleem – zelfs als niet vaststaat dat het gekozen middel überhaupt werkt – is heel sterk in politieke en beleidskringen. Er kunnen drie factoren worden onderscheiden die ertoe leiden dat onbewezen 'oplossingen' centraal komen te staan en een panacee worden voor een waaier aan problemen. Ten eerste is er voor politici de druk om bestuurlijke daadkracht te tonen en met een concrete maatregel de media te halen; ten tweede is er vaak zoveel energie gestoken in een bepaalde oplossing dat er een punt van no return is bereikt; en ten derde spelen er ook andere, financiële belangen bij de keuze voor een bepaalde beleidsmaatregel (WODC, 2011, p. 6).

Een recent voorbeeld van de neiging tot function creep komt van de Belastingdienst, die inzage eiste bij de databank van de Stichting Museumjaarkaart om aan te tonen dat iemand niet in Nederland woont (Weijts, 2018). Tegelijk gaf diezelfde Belastingdienst overigens ook aan persoonlijke gegevens niet goed te kunnen beschermen (Kleinnijenhuis, 2018). Het is overigens maar de vraag of function creep zinvol is voor overheden, omdat data die uit hun context worden gehaald en in een nieuwe context wor-

den hergebruikt, minder betrouwbaar kunnen zijn (WODC, 2011, p. 17).

Profilering

De tweede keerzijde van transparantie is dat bedrijven data kunnen opvragen die wellicht weer terug te herleiden zijn tot persoonlijke gegevens. Als gegevens eenmaal gedeeld zijn, valt niet meer te achterhalen waar deze terecht komen en hoe ze gebruikt worden bij het ontwikkelen van producten en diensten. Dat kan lelijk uitpakken, zo heeft wiskundige Cathy O'Neil aangetoond in haar boek *Weapons of Math Destruction*. Zij beschrijft daarin hoe uit oogpunt van winstmaximalisatie bedrijven proberen om hun klanten zo nauwkeurig mogelijk te categoriseren in doelgroepen. Zo kunnen bedrijven onevenredig veel invloed uitoefenen op het leven van mensen, zelfs zonder dat deze mensen zich hiervan bewust zijn. Bijvoorbeeld doordat bedrijven bepalen welke informatie, keuzes, dienstverlening of producten mensen wel of niet krijgen en in welke kwaliteit en voor welke prijs. Dit kan de keuzevrijheid van mensen belemmeren, mensen discrimineren en uitsluiten, en de sociaaleconomische ongelijkheid vergroten (O'Neil 2017).

De AVG verbiedt profilering niet, zo lang de impact op de privacy beperkt is. Het zal voor consumenten echter lastig zijn om negatieve effecten te herkennen en te bestrijden, al dan niet via de juridische weg. Mensen zijn zich immers vaak niet eens bewust van het feit dat hun gegevens zijn gebruikt, laat staan op welke wijze. En bedrijven hoeven hun business model niet snel prijs te geven, omdat het onder hun intellectueel eigendomsrecht kan vallen.

Overheden zijn zich overigens van deze mogelijke negatieve gevolgen van het delen van data bewust. Zo adviseert de VNG in haar 'Handreiking Wet hergebruik overheidsinformatie' aan de gemeenten om informatievragers te informeren over de mogelijke risico's van hun handelen op dit gebied (Bulut-Keskin, 2018, p. 9). Dit advies van de VNG strekt zich echter niet uit tot de burgers wiens gegevens doorgespeeld worden. Zij blijven onbewust van wat er gebeurt.

Dataminimalisatie

Hoe kunnen overheden enerzijds transparant zijn en de data waarover ze beschikken openbaren en delen, en anderzijds de privacy van burgers zoveel mogelijk beschermen? Een oplossing is om zo min mogelijk data te verzamelen die persoonlijk is of de potentie in zich draagt persoonlijk te worden. Overheden zouden het eerder genoemde artikel 25 van de AVG (over 'gegevensbescherming door ontwerp en door standaardinstellingen') in ieder geval zo strikt mogelijk moeten toepassen, óók op gegevens die later geanonimiseerd zullen gaan worden. Overheden zouden niet de alleen de vraag moeten stellen: 'welke data heb ik nodig voor de taakuitvoering?' maar ook de vraag 'kunnen we onze taken uitvoeren zonder deze data te verzamelen?'

Het nadeel van dataminimalisatie is dat het lastiger wordt om onderzoek te doen, bijvoorbeeld op het gebied van volksgezondheid. Momenteel worden persoonlijke data verzameld en geanonimiseerd om ze geschikt te maken voor analyse. Deze data zouden er in het geval van dataminimalisatie domweg niet meer zijn. De oplossing hiervoor ligt bij de burger zelf, als deze zelf kan bepalen of hij persoonlijke gegevens wil delen ten behoeve van een specifiek doel. Dit zou het ultieme 'zeggenschap over data' zijn, wat een van de uitgangspunten is van het Amsterdamse manifest Tada.

Onderzoeksinstituut Waag is, in samenwerking met andere partijen, met deze vorm van zeggenschap aan het experimenteren. Het heeft hiertoe het project ' DECODE' in het leven geroepen (Waag, 2018). Met behulp van nieuwe technieken[4] biedt DECODE burgers controle over welke gegevens ze over zichzelf willen prijsgeven binnen 'data commons' (dataplatformen voor gemeenschappelijk gebruik), waarbij de betrokken burgers gezamenlijk de regels voor toegang en gebruik ervan opstellen. Eenmaal vrijgegeven data blijven traceerbaar voor de datadeler.

4 Deze technieken zijn gebaseerd op basis van blockchain en autorisatie met behulp van een digitale identiteit. Blockchain is een digitaal systeem om gegevens vast te leggen. Omdat er niet één beheerder is, maar meerdere die elkaar controleren, is het vervalsen van de vastgelegde gegevens niet mogelijk.

Een mogelijk probleem met projecten als DECODE is wel dat het naar verwachting lastig zal worden om een significant deel van de Nederlandse burgers te betrekken. Het Rathenau Instituut zoekt de oplossing voor dit type probleem in het 'stimuleren van technologisch burgerschap' en omschrijft dit als volgt:

> Een 'technologisch burger' is geïnformeerd over de werking van technologie, kan kritisch nadenken over die werking en de betekenis daarvan voor zijn leefwereld, en kan op basis daarvan kiezen welke technologie hij wel of niet kan of wil gebruiken. Dat betekent bijvoorbeeld dat mensen begrijpen hoe profilering en zelflerende algoritmen werken en hoe dat hen beïnvloedt, en dat ze in staat zijn zich te verweren tegen ongewenste invloeden, en alternatieven kunnen kiezen. Technologisch burgerschap vraagt daarom om het vergroten van het maatschappelijk bewustzijn en het stimuleren van de meningsvorming over de invloed en betekenis van de nieuwe digitaliseringsgolf (Kool, Timmer, Royakkers & Van Est, 2017, p.16).

De hoop is bij het Rathenau instituut dus gevestigd op betere scholing van de burger. Het is echter maar zeer de vraag of de burger deze hoge verwachtingen waar kan maken. Ondanks alle inspanningen van ons onderwijs tot nu toe, is nog steeds ca. 2,5 miljoen volwassenen laaggeletterd en/of laaggecijferd (Algemene Rekenkamer, april 2016). Deze groep heeft vaak ook moeite met digitale vaardigheden. Daarbij heeft de Wetenschappelijke Raad voor het Regeringsbeleid laten zien dat een groot deel van de bevolking dat wél geletterd is, moeite heeft met het maken van keuzes of het zelf inrichten van zijn leven (WRR, 2017, p. 19). Volgens de WRR geldt dit zelfs voor veel goed opgeleide burgers: "Er bestaat een behoorlijk verschil tussen wat van burgers wordt verwacht en wat zij daadwerkelijk aankunnen. De helft van alle Nederlanders (48 procent) heeft bijvoorbeeld moeite om zelf de regie te voeren over gezondheid, ziekte en zorg. Het ontbreekt hen aan kennis, motivatie en zelfvertrouwen." (WRR, 2017, p. 19). De WRR spreekt in dit verband over 'doenvermogen' naast 'denkvermogen' (WRR, 2017, pp. 10-12). Doenvermogen vereist volgens de WRR actiebereidheid, doorzettingsvermogen en de kunst om niet te bezwijken onder verleidingen of keuzestress. Het is maar een selecte groep Nederlanders die over dat doenvermogen beschikt, volgens de WRR. Het is mijns inziens niet te verwachten dat de burger zonder doenvermogen zich tot 'technologisch burger' zal ontwikkelen. En van de burgers die wel over denk- én doenvermogen beschikken, zal een deel afhaken wegens tijdgebrek of desinteresse.

Bij DECODE komt daar nog bij dat het gaat om belangeloze participatie, en dat de keuze om data vrij te geven voor een specifiek doel steeds opnieuw – tot vermoeiens toe - herhaald zal moeten worden, omdat data nu eenmaal snel verouderen. Daar staat weer tegenover dat er technische oplossingen in de maak zijn die mensen controle geven over welke data ze in welke situatie vrijgeven. Uiteraard is dit ook algoritmisch te regelen. Het gevaar blijft echter dat initiatieven als DECODE een speeltje blijven van een kleine groep professionals met denk- en doenvermogen én interesse in de materie.

Concluderend

Er is sprake van een spanningsveld tussen privacy en transparantie waar het overheidsdata betreft. Transparantie is belangrijk uit oogpunt van democratische controle, bijvoorbeeld om te zien welke gegevens overheden verzamelen en hoe ze hiermee omgaan. Ook kan gecontroleerd worden of deze data accuraat, geschikt en betrouwbaar zijn en of ze rechtmatig verkregen zijn. Transparantie is ook belangrijk uit oogpunt van waardecreatie. Er is dan ook wetgeving die overheden verplicht stelt data te openbaren en te delen. De AVG verplicht overheden en private partijen daarbij om het grondrecht van privacy te waarborgen. Persoonlijke data die gedeeld worden, zouden geanonimiseerd moeten zijn, bijvoorbeeld via aggregatie. Maar door het combineren van databases is informatie mogelijk weer te herleiden tot personen, dus dit is niet waterdicht. Verder geldt het doelbindingsprincipe van de AVG bij datadeling. Dit is echter met de juiste argumenten te omzeilen, bijvoorbeeld

voor opsporingsdoeleinden. Daarbij stelt het WODC dat overheden van nature geneigd zullen zijn om de ruimte te benutten die hiermee wordt geboden.

Al met al blijkt het waarborgen van zo groot mogelijke privacy behoorlijk ingewikkeld, zelfs nu er een AVG is. Wat in ieder geval helder is, is dat een overheid die de privacy van haar burgers serieus neemt, geen genoegen kan nemen met het simpelweg opdelen van gegevens in 'persoonlijke gegevens' en niet-'persoonlijke gegevens' en de oplossing voor het privacy-probleem zoeken in het aggregeren van de persoonsgegevens. Overheden zullen moeten gaan nadenken over wat het combineren van verschillende categorieën gegevens – van henzelf, maar ook van andere overheidsinstellingen of van bedrijven - potentieel kan betekenen. Artikel 25 zou dan sowieso altijd toegepast moeten worden, of gegevens nou gepseudonimiseerd of geanonimiseerd worden. Het is dan bovendien aan de gemeenteraden en Provinciale Staten om er vanuit hun kaderstellende en controlerende rol op toe te zien dat het maximum gehaald wordt uit principes als dataminimalisatie en *acces control*. Het draait hierbij vooral om de verantwoording door de bestuurders. En de beste verantwoording laat niet alleen zien waarom welke keuzes gemaakt zijn, maar ook waarom de verdergaande keuzes níet gemaakt zijn. Dit laatste wordt vaak vergeten.

5. Het verwerken van gegevens via algoritmen

Computerprogramma's verwerken de (big) data die ingevoerd worden tot bepaalde uitkomsten. Hiervoor gebruiken ze algoritmen, ofwel series van instructies. Op deze wijze kunnen overheden hun taken vaak sneller en gemakkelijker uitvoeren. Maar algoritmen zijn niet altijd objectief. Ook kunnen algoritmen zeer ingewikkeld worden. In hoeverre groeien de algoritmen ons straks boven het hoofd?

Algoritmen worden steeds beter in wat ze doen
Algoritmen kunnen werken volgens het principe van een beslisboom: "Als a gebeurt, dan b. Als a niet gebeurt, dan c". In andere gevallen is er geen sprake van een beslisboom, maar werkt het algoritme als een neuraal netwerk, net zoals onze hersenen.[5] We spreken dan van 'Kunstmatige Intelligentie' of 'Artificial Intelligence'. Dit soort algoritmen zijn vooral goed in het opsporen van patronen in data en het op basis daarvan doen van voorspellingen.

Het verwerken van data kan dus op verschillende manieren, afhankelijk van het type algoritme. Het classificeren en combineren van data wordt momenteel toegepast bij het zogeheten *predictive policing* (Dubbeld, 2017). De politie combineert bepaalde data (bijvoorbeeld de samenstelling van de bevolking, de ruimtelijke kenmerken van een wijk, het aantal criminele feiten en het aantal veelplegers) en bepaalt op basis daarvan waar in welke mate gesurveilleerd moet worden. Zo meent de politie haar werk efficiënter te kunnen uitvoeren. De gemeente Kerkrade gebruikt een algoritme dat voorspelt in welke straten de meeste kans is op eenzaamheid (Hartholt, 2017).

En de Amsterdamse en Groningse GGD's onderzochten in 2015 of een computer via *text mining* (het doorploegen van eindeloze hoeveelheden informatie uit dossiers) kon identificeren welke kinderen een hogere kans hadden om mishandeld te worden binnen hun gezin (NCJ, 2018).

Het voordeel van computers is dat deze onvermoeibaar zijn in het snel verwerken van eindeloze hoeveelheden informatie en het ontdekken van patronen in gegevens. Vervolgens worden ze daar bovendien steeds beter in. Zo worden computers met behulp van grote hoeveelheden data getraind om bepaalde taken uit te voeren. Dit heet '*machine learning*'. Er zijn computers die aan een specifieke vorm van machine learning doen, namelijk '*deep learning*'. Deep learning houdt in dat de computer abstracte begrippen en concepten kan leren zonder dat hier nog een menselijke interventie voor nodig is. Het algoritme achter deep learning is gebaseerd op patroonherkenning en het verwerken van data op verschillende niveaus. Na voldoende voorbeelden 'weet' de computer hoe een konijn, of welk ander willekeurig object dan ook, eruitziet en kan het die ook in nieuwe foto's en video's aanwijzen. Dus zoals een peuter het concept 'konijn' kan leren en zo ieder konijn kan herkennen – zelfs een wat afwijkend konijn met drie poten, zonder oor of kaal – kan een computer ook zulke concepten aanleren.

In bijvoorbeeld de medische wereld wordt dit van steeds groter belang (Schuurmans, 2018). Na eindeloos veel input, denk aan foto's van oogziektes, zal een computer met behulp van een algoritme zelf kunnen leren om bijvoorbeeld om zelf oogziektes te herkennen. Hetzelfde zal gelden voor tumoren: op basis van het samenspel van kleuren, vormen en contouren zal de computer deze kunnen herkennen, ook al ziet een tumor er net iets anders uit dan de oorspronkelijke beschrijving ervan. Omdat computers onvermoeibaar zijn en ook kleine afwijkingen waarnemen, zullen ze dit naar verwachting uiteindelijk beter kunnen dan de mens.

Een andere vorm van machine learning is '*reinforcement learning*'. In de Engelse krant *The Guardian* staat helder uitgelegd hoe dat werkt, aan de hand van een voorbeeld over een casino. Hierbij is een algoritme geprogrammeerd om zodanig te spelen dat het altijd voor de

5 Dit essay gaat niet in op de werking van zo'n neuraal netwerk, aangezien het complexe materie is die erg veel uitleg vereist. Een heldere uitleg is te vinden op: https://www.passionned.nl/bi/predictive-analytics/neuraal-netwerk/

hoogste score gaat. Het algoritme 'leert' door snel miljoenen spellen te spelen en de positieve en negatieve leerervaringen te verwerken. Dit is reinforcement learning. Op het moment dat een algoritme zo zélf leert, weten wij als mensen niet meer van welke data of codes het algoritme gebruik maakt. Daarbij kunnen algoritmen gecodeerd zijn om op elkaar te reageren, zoals bijvoorbeeld inmiddels op de aandelenbeurs gebeurt. Door de ingewikkelde interactie die hierdoor ontstaat heeft de mens geen inzicht meer in of controle meer over het proces danwel de uitkomst (Smith, 2018).

De tekortkomingen van algoritmen

Waar het mis gaat met algoritmen, is ten eerste in de veronderstelling dat de uitkomsten van algoritmen objectief zouden zijn. Dit in tegenstelling tot menselijke oordelen, die impliciete vooroordelen omvatten. Wat dan wordt vergeten, is dat de kwaliteit van de gebruikte gegevens onder de maat kan zijn, of dat menselijke vooroordelen kunnen meespelen bij het gebruik van gegevens of in het coderen van het algoritme, net zoals een smaakvoorkeur onbewust kan meespelen bij het opstellen van een recept. Om dit te doorbreken is het nodig om bloot te leggen welke of welk type gegevens worden gebruikt, hoe een algoritme is opgebouwd en vooral wat de vooronderstellingen zijn.

De eerder genoemde wetenschapper Cathy O'Neil geeft talloze voorbeelden van de tekortkomingen van algoritmen (O'Neil, 2017). Het begint bij gebruikmaking van data die onjuist, verouderd of ongeschikt zijn, iets wat een algoritme niet ondervangt. Vervolgens kan het verkeerd gaan bij de codering. Het volgende voorbeeld uit haar boek laat zien hoe dit werkt: bij een algoritme om de kans op recidive te bepalen, werd uitgegaan van de mate waarin men in aanraking was gekomen met de politie vóórdat de misdaad plaatsvond waarvoor men bestraft was. Aangezien zwarte mensen in de VS door vooroordelen vaker staande worden gehouden dan witte, had het algoritme als uitkomst dat zwarten vaker zouden recidiveren dan witte mensen (O'Neil, 2017).

Daarnaast creëren algoritmen soms zogenoemde 'feedback loops'. Als bijvoorbeeld uit analyse blijkt dat er op bepaalde plekken meer misdaad voorkomt, zal de politie daar meer surveilleren. Daardoor signaleert de politie vooral de misdaad op die plek, met als gevolg dat de plek een volgende keer nog hoger scoort in de statistieken. Ondertussen komt het werk van de politie op andere terreinen in het gedrang. (O'Neil, 2017). Zo kan het algoritme een vicieuze cirkel creëren waarin steeds het eigen gelijk bevestigd wordt en waar onbedoeld negatieve effecten ontstaan. Het algoritme schiet uiteindelijk zijn doel voorbij.

Een ander probleem met algoritmen is dat de uitkomsten ervan ongrijpbaar kunnen zijn. Dan is niet of nauwelijks meer te begrijpen hoe de uitkomst samenhangt met de input. Dat kan te maken hebben met de complexiteit van de beslisboom waarbij verschillende algoritmen en vele categorieën data gebruikt worden, maar ook met het eerder genoemde machine learning. Dit leidt tot vervreemding, het onprettige gevoel dat de mens ongewild geen invloed meer heeft op ontwikkelingen die hem of haar wél raken. Transparantie en *accountability* zijn dan bovendien ver te zoeken. In het geval dat een overheid zo'n soort algoritme toepast, zal dit ongetwijfeld leiden tot minder vertrouwen in de overheid.

Tot slot wordt zowel het gebruik als de codering van algoritmen soms bewust geheim gehouden, bijvoorbeeld als ze gebruikt worden voor opsporingsdoeleinden. Een voorbeeld hiervan is bijvoorbeeld dat als bekend zou worden dat het gegeven 'leegstaande kas' gebruikt wordt in het algoritme dat probeert te voorspellen waar grotere kans is op wietteelt, criminelen hierop kunnen reageren door uit te wijken naar leegstaande fabriekshallen. Hier is dus sprake van een spanningsveld tussen opsporing en transparantie. Want hoe controleer je dan nog of een algoritme geen ongewenste bijwerkingen heeft, bijvoorbeeld als het gaat om bijstandsuitkeringen? Tweede Kamerlid Rens Raemakers stelde in april 2018 dan ook Kamervragen over de algoritmen die gebruikt worden om bijstandsfraude op te sporen (Tweede Kamer der Staten Generaal, 2018). Kamerleden Verhoeven en Buitenweg hebben in dit kader op 6 juni 2018 een motie ingediend waarin de regering werd verzocht de door de overheid gebruikte algoritmen zoveel mogelijk te openbaren (Kamerstuk, 2018). Minister Dek-

ker heeft toegezegd dat hij begin 2019 met een antwoord zal komen en dat ook de EU begin 2019 met een voorstel betreffende ethiek en kunstmatige intelligentie zal komen (Kamerbrief, 2018).

Bescherming tegen uitwassen

Kortom, er schuilt gevaar in het gebruik van algoritmen. In principe kan het gebruik van algoritmen leiden tot efficiëntere en effectievere overheidstaakuitvoering en bijdragen aan 'goed openbaar bestuur'. Maar onjuist gebruik of bijwerkingen kunnen juist het tegenovergestelde bewerkstelligen. Bovendien, zo laten talloze voorbeelden zien, staan beginselen als transparantie, accountability en gelijke en eerlijke behandeling van burgers op het spel.

De bestaande wet- en regelgeving stelt wel enige eisen aan de verwerking van data, en daarmee aan algoritmen. In artikel 5 staat dat gegevensverwerking 'rechtmatig, behoorlijk en transparant' moet gebeuren. Artikel 12 voegt daaraan toe dat die verplichte uitleg in helder en begrijpelijk Nederlands moet zijn. Artikel 13.2f geeft aan dat overheden burgers op de hoogte moeten stellen als hun data verwerkt worden tot een geautomatiseerde besluit. Artikel 22 geeft mensen het recht om niet onderworpen te worden aan profilering. En in artikel 18, tot slot, staat dat de eenieder het recht heeft om bezwaar te maken tegen de verwerking van hem betreffende persoonsgegevens of tegen profilering, maar alleen als er geen correcte gegevens gebruikt worden of als de verwerking onrechtmatig is.

Bij bestuurlijke besluiten kan de burger de overheid sowieso houden aan de algemene beginselen van behoorlijk bestuur (abbb), de deels in jurisprudentie vastgestelde gedragsregels van de overheid ten opzichte van de burger. Zo vereist het zorgvuldigheidsbeginsel het gebruik van correcte gegevens, en het motiveringsbeginsel vereist transparantie, bijvoorbeeld over welke algoritmen waar en wanneer met welk doel door een overheid worden gebruikt. Bovendien moet zo'n algoritme uitlegbaar zijn.

Deze wet- en regelgeving lost problemen omtrent onjuiste aannames, bias of verkeerd gelegd verbanden echter niet op. Ook hoeven overheden volgens de AVG en abbb geen transparantie te betrachten als er algoritmen worden gebruikt die niet tot een besluit leiden. Volgens de Code goed openbaar bestuur zou dat overigens uit oogpunt van transparantie en accountability wel wenselijk zijn. Als overheden samenwerken met bedrijven geldt het bijkomend probleem dat bedrijven hun algoritme niet hoeven te openbaren uit concurrentieoverwegingen.

Als reactie op dit probleem is recent door politici voorgesteld om een 'waakhond' op te richten om algoritmes en de onderliggende datasets te controleren om te zien of er sprake is van discriminatie of privacyschending. Deze waakhond zou dan bij de ACM of de Autoriteit Persoonsgegevens moeten worden ondergebracht (Hartholt, 2018). Enerzijds is het logisch om de kennis en expertise die nodig is om algoritmen te controleren bij elkaar te brengen, anderzijds is het niet logisch om iedere simpele rekenregel aan een waakhond of toetsingscommissie voor te leggen. Wat mijns inziens eerst nodig is, is een afweging welke algoritmen wel en niet in aanmerking komen voor externe controle. Daarvoor moet een algoritme overigens wel controleerbaar ofwel 'auditbaar' zijn. Vervolgens kan bekeken worden hoe zo'n controle of audit er dan uit zou moeten zien.

Onuitlegbare en oncontroleerbare algoritmen

Het is een probleem dat algoritmen steeds ingewikkelder worden en daarmee moeilijker te begrijpen of uit te leggen. Dit geldt volgens Mona de Boer, wetenschappelijk onderzoeker bij de Universiteit van Amsterdam, vooral voor algoritmen die werken als een neuraal netwerk (persoonlijke communicatie, 18-10-2018). Dit bemoeilijkt het opstellen van begrijpelijke zogeheten 'algoritme-bijsluiters', die weleens als oplossing wordt aangedragen (Van der Wel, 2015). 'Moeilijk uitlegbaar' betekent echter niet meteen 'oncontroleerbaar'. Universiteiten en accountancybedrijven zijn instrumenten aan het ontwikkelen waarmee algoritmen gecontroleerd kunnen worden. Cathy O'Neil, de wetenschapper die al eerder de impact van algoritmen op het leven van gewone Amerikanen zichtbaar maakte, heeft als een van de eersten zo'n tool ontwikkeld (Hempel, 2018; Wielaard, 2018).

En aan de UvA wordt een instrument ontwikkeld dat niet alleen zelflerende algoritmen zou moeten controleren, maar dat ook inzicht moet geven in welke algoritmen 'auditbaar' zijn en welke niet, ervan uitgaande dat dat bij sommige algoritmen op enige termijn niet meer het geval zal zijn (ContentWorks, 2018). Over pakweg vijftien jaar zal er dus sprake zijn van een driedeling in algoritmen: ten eerste algoritmen waarvan de uitkomsten uitlegbaar én controleerbaar zijn, ten tweede algoritmen die niet goed uitlegbaar zijn maar nog wel controleerbaar, en ten derde algoritmen die ook niet meer controleerbaar zijn.

Daarbij noemt minister Dekker in zijn brief aan de Tweede Kamer nog een onderbelicht knelpunt dat de transparantie over algoritmen belemmert, namelijk de hoge uitvoeringskosten als alle algoritmen – ook de ingewikkelde - geopenbaard en uitgelegd moeten worden (Kamerbrief, 2018, p. 4). Als algoritmen ingezet worden om (controleerbare) algoritmen te controleren, wordt dit echter wellicht deels opgelost.

Een afweging met betrekking tot algoritmen

Computers kunnen besluiten nemen, maar dat wil niet zeggen dat ze er verantwoordelijk voor zijn. De overheid blijft verantwoordelijk voor haar besluitvorming, de wijze waarop deze tot stand is gekomen en de wijze waarop deze haar burgers raakt. Gemeenteraden en Provinciale Staten hebben een kaderstellende, controlerende en volksvertegenwoordigende taak. Als een gemeente, provincie of een door hen gemandateerde uitvoeringsorganisatie algoritmen gebruikt bij haar taakuitvoering, ligt de verantwoordelijkheid voor het bepalen van de randvoorwaarden en de controle erop dan ook in de eerste plaats bij de volksvertegenwoordiging. Het dagelijks bestuur moet inzicht geven in en verantwoordelijkheid afleggen over het gebruik (*accountability*).

In dit kader gaat bijvoorbeeld de Provincie Noord-Holland ervan uit dat de overheid een keuze heeft tussen datagedreven handelen, waarbij denkende mensen de beslissingen nemen op basis van informatie die door data en algoritmen gegenereerd is, en datagestuurd handelen, waarbij de uitkomsten van data en algoritmen klakkeloos worden overgenomen. In de Datastrategie van deze provincie wordt vervolgens de keuze gemaakt voor datagedreven handelen (Provincie Noord-Holland, 2018b, p.4). Dit is in overeenstemming met het principe van Tada: 'de menselijke maat blijft leidend'. Het Tada-manifest en Provincie Noord-Holland gaan echter uit van de algoritmen die wij nu kennen, welke vaak nog relatief eenvoudig zijn. Maar hoe gaan ze straks om met de zeer ingewikkelde en oncontroleerbare algoritmen die bijvoorbeeld binnen het Internet of Things zullen worden toegepast? Algoritmen die misschien wel gebruik maken van duizenden variabelen? Of van deep learning?

Uiteraard kan een overheid zich voornemen om geen ingewikkelde algoritmen toe te passen. Maar doet die overheid de maatschappij dan niet tekort? Algoritmen zijn nodig om op termijn de kansen die in dit essay zijn geschetst, te benutten. Daarbij hebben we gezien dat er naar verwachting sprake zal zijn van grote maatschappelijk druk op overheden om 'mee te digitaliseren' met de maatschappij en efficiënter en effectiever te werken.

Het is wellicht zinvoller voor overheden om bewuste keuzes te maken: wanneer willen we datagedreven handelen en wanneer willen we datagestuurd handelen? Wanneer willen we dat een algoritme technisch uitlegbaar en controleerbaar is, en wanneer vinden we het voldoende als alleen de uitkomst van een algoritme verklaard kan worden? En voor wie moet een en ander dan uitlegbaar of verklaarbaar zijn, voor specialisten of voor burgers? Uiteraard betekent een keuze voor uitlegbare algoritmen wel dat maatschappelijke kansen soms ook gemist zullen worden.

Wat hebben gemeenteraden en Provinciale Staten dan nodig om te bepalen aan welke randvoorwaarden welk type algoritme moet voldoen om toegepast te mogen worden in beleids- en besluitvorming? Het zal in ieder geval gaan om:

1. Inzicht in waar en wanneer algoritmen gebruikt gaan worden voor de taakuitvoering. Dit geldt uiteraard ook voor samenwerkingspartners, uitvoeringsdiensten en private opdrachtnemers;
2. Inzicht in doel en beoogd maatschappelijk effect van het inzetten van algoritmen: gaat

het om beleidssturing of om besluiten? Gaat het om objecten, de leefomgeving of om burgers? Raken besluiten burgers direct of indirect?

3. Of algoritmen eenvoudig of complex zullen (moeten) zijn om bepaalde taken efficiënt en effectief uit te kunnen voeren.

Het algoritme impact assessment

Nadat bepaald is welk type algoritmen waar toegepast mogen worden, kunnen gemeenteraden en Provinciale Staten gaan bepalen welk typen algoritmen in aanmerking komen voor toetsing of een algoritme wel 'eerlijk' en 'rechtvaardig' is. Het zal dan naar verwachting vooral gaan om algoritmen met een grote potentiële impact op het leven van burgers.

Wetenschappers van het AI Institute van New York University hebben zich verdiept in hoe zo'n controle eruit zou kunnen zien (Reisman, Schultz, Crawford & Whitaker, 2018a; 2018b). Zij hebben aanbevelingen opgesteld voor een 'algoritme impact assessment'. Elementen zijn onder meer het betrekken van externe deskundigen om de methodes en effecten op langere termijn te evalueren, transparantie over het algoritmebeleid zodat ook de burger er kennis van kan nemen, het betrekken van overheidsinstanties die de expertise hebben om de gevolgen van beleid in beeld te brengen en het bieden van de mogelijkheid aan de burger om bezwaar in te dienen tegen het gebruikte algoritme. Volgens deze wetenschappers zijn deze onderdelen absoluut nodig om ervoor te zorgen dat de burger vertrouwen houdt in de overheid. Daarbij hoort volgens dezelfde wetenschappers ook dat overheden die bedrijven inschakelen bij hun taakuitvoering, contractueel kunnen vastleggen hoe de accountability van algoritmes geborgd wordt, en dat bedrijven daarmee hun recht op bedrijfsgeheim soms zullen moeten verwerpen om een overheidsopdracht in de wacht te kunnen slepen (Reisman et al, 2018b, p. 14).

In de aanbevelingen van de wetenschappers van NYU zien we aspecten terug die eerder in dit essay aan de orde zijn gekomen, zoals de 'waakhond' (externe deskundigen) en de technologisch geschoolde burger. Hoewel we hebben gezien dat slechts een kleine groep burgers in staat wordt geacht zich tot 'technologisch burger' te ontwikkelen, is het wel van belang dat deze burgers hiertoe de kans krijgen en hierin ondersteund worden, zodat zij de burgers kunnen vertegenwoordigen die hiertoe niet in staat zijn. Dit vergroot de democratische legitimatie van de toepassing van algoritmen. Bovendien is het in het gemeentelijk sociaal domein van belang dat de ervaringskennis van burgers en cliëntorganisaties wordt meegenomen om effecten in te schatten.

Concluderend

Algoritmen kunnen overheden helpen hun taken efficiënter en effectiever uit te voeren. Het gebruik van algoritmen is echter niet onomstreden, en wel om verschillende redenen. Algoritmen zijn niet altijd objectief, omdat het type en de kwaliteit van de gegevens of indicatoren die de mens als input selecteert, de uitkomst mede bepaalt. Hetzelfde geldt voor de codering, waarin vooroordelen een rol kunnen gaan spelen. Als overheden niet transparant zijn over de gebruikte algoritmen, en over het gebruik ervan geen verantwoording hoeven af te leggen, blijven problemen met algoritmen verborgen. De AVG en abbb lossen deze problemen niet altijd op, want overheden hoeven volgens de AVG en abbb geen transparantie te betrachten als er algoritmen worden gebruikt die niet tot een besluit leiden. Als overheden samenwerken met bedrijven geldt het bijkomend probleem dat bedrijven hun algoritme niet hoeven te openbaren uit concurrentieoverwegingen.

Deze problemen zouden opgelost kunnen worden, bijvoorbeeld via controlerende algoritmen, ware het niet dat algoritmen op termijn dusdanig ingewikkeld kunnen worden, dat controle onmogelijk wordt. Uiteraard kan een overheid zich voornemen om geen ingewikkelde algoritmen te gebruiken, maar dan loopt de overheid kansen mis. Het is daarom zinvol voor overheden om keuzes te maken in wanneer een algoritme verklaarbaar, technisch uitlegbaar of controleerbaar zou moeten zijn, en wanneer dat niet nodig is. Bij algoritmen met potentieel grote impact op het leven van burgers zou bovendien een impact assessment gedaan kunnen worden.

Zonder Europese en rijksregelgeving op dit vlak, is het aan de gemeenteraden en Provinciale Staten om hier vanuit hun kaderstellende rol keuzes in te maken. De consequentie van dit alles is wel dat er soms kansen onbenut zullen blijven. Transparantie en 'de menselijke maat' zullen dan boven efficiëntie en/of effectiviteit gaan. Het is mijns inziens aan gemeenteraden en Provinciale Staten om over deze keuzes verantwoording af te leggen aan de burger.

6. Conclusies en aanbevelingen

Het samenspel van sensortechnologie, big data, algoritmen en IoT biedt grote kansen voor de maatschappij op het gebied van welvaart en welzijn, maar kan ook negatieve gevolgen hebben. Hoe kunnen overheden op integere wijze met deze technologieën omgaan en wat betekent dat voor de manier waarop ze zouden moeten gaan werken en georganiseerd zijn?

Publieke waarden in het geding

Veel overheden hebben de mogelijkheden die de Vierde Industriële Revolutie biedt, enthousiast omarmd. Er wordt immers volop geëxperimenteerd met het vergaren, openbaren, delen, verwerken en gebruiken van (big) data, bijvoorbeeld via sensortechnologie en bij het Internet of Things. Als er al besef is van het feit dat dit mogelijk tot aantasting van publieke waarden leidt, dan blijft het vaak abstract waar die aantasting zich precies voordoet en welke mogelijke oplossingen er zijn. In dit essay is geprobeerd dit te concretiseren en inzichtelijk te maken. Zo'n concretiseringsslag zou wat mij betreft ook plaats moeten vinden voor andere technologieën waarmee overheden aan het experimenteren zijn, zoals bijvoorbeeld virtual reality en blockchain.

Bij het vergaren, openbaren, delen, verwerken en gebruiken van (big) data blijken publieke waarden als persoonlijke vrijheid en bescherming tegen te grote machtsuitoefening door de overheid in het geding. Deze waarden komen tot uiting in diverse grondrechten en beginselen. Monitoring in de openbare ruimte bedreigt de keuzevrijheid. Bij gedragssturing op basis van data dreigt manipulatie. Bij profilering op basis van data met behulp van algoritmen dreigt discriminatie. En als algoritmen bij beleids- en besluitvorming worden gebruikt, moeten deze uit oogpunt van accountability en democratische controle uitlegbaar en controleerbaar zijn. Het zal steeds moeilijker worden om aan deze vereisten tegemoet te komen.

(Deel)oplossingen

In dit essay zijn allerlei (deel)oplossingen aangedragen voor bovengenoemde problemen, zoals:

- Een sensordataregister, waardoor inzichtelijk wordt welke overheid welk type data in de openbare ruimte vergaart. Dit vergroot de transparantie. Dit lost het probleem van verminderde keuzevrijheid om onbespied te gaan en staan waar men wil, echter nog niet op. Om te voorkomen dat hele gemeenten onbegaanbaar worden voor burgers die niet van monitoring gediend zijn, dient een afweging gemaakt te worden tussen algemeen belang en individueel belang. Deze afweging kan alleen door de volksvertegenwoordiging gemaakt worden. Nut en noodzaak van datavergaring moeten dan wel uiterst kritisch beoordeeld worden.
- In situaties waarin het praktisch gezien ondoenlijk is om expliciet de toestemming van iedere burger te vragen voor datavergaring- of verwerking, of waar verwacht wordt dat burgers door de bomen het bos niet meer zullen zien, zou die toestemming in ieder geval bij de volksvertegenwoordiging opgehaald moeten worden.
- Er zijn maatstaven ontwikkeld voor gedragssturing, opdat dit niet uitmondt in manipulatie. Deze maatstaven moeten dan uiteraard wel gehanteerd worden. Gemeenteraden en Provinciale Staten kunnen hierop sturen vanuit hun kaderstellende en controlerende rol.
- De AVG is ingesteld om de privacy te beschermen. Helaas is de AVG niet 'waterdicht' en op termijn – als bijna alle data 'persoonlijke data' worden – steeds minder houdbaar. Alleen vergaande dataminimalisatie en acces control kunnen aantasting van de privacy helpen voorkomen. Hier zijn technische hulpmiddelen voor in ontwikkeling. Dataminimalisatie bemoeilijkt echter weer wetenschappelijk onderzoek. Als oplossing hiervoor is bedacht dat burgers zelf zouden moeten kunnen bepalen in welke situatie ze persoonlijke gegevens willen vrijgeven. De vrees is echter dat slechts een kleine groep burgers hierin geïnteresseerd zal zijn.

- Het ontwikkelen van 'technologisch burgerschap' zou burgers weerbaar maken tegen de invloeden van digitalisering. Hier mogen we mijns inziens echter niet te veel van verwachten. Ten eerste vereist zo'n ontwikkeling een denk- en doenvermogen dat veel mensen ontberen, ten tweede zullen juist de zelflerende algoritmen straks ook voor experts niet goed meer te volgen zijn. Niettemin is het belangrijk dat de burgers die er wél enigszins toe in staan zijn, de kans krijgen zich hierin te ontwikkelen zodat zij kunnen participeren en de kar kunnen trekken voor hen die dat niet kunnen. Het is dan wel aan gemeenteraden en Provinciale Staten om ervoor te zorgen dat het algemeen belang geborgd blijft.
- Tot slot is een toezichtscommissie of 'waakhond' genoemd voor controle op ingewikkelde algoritmen en hun effecten. Zo'n kennisbundeling van expertise lijkt me nuttig en nodig, maar dit vereist dan wel eerst een afweging binnen overheidsorganisaties in welke beleidsvelden welk type algoritmen ingezet mogen worden en welke extern beoordeeld zouden moeten worden. Niet iedere simpele rekenregel of beslisboom behoeft immers het oordeel van een aparte toezichtcommissie. Vragen die beantwoord moeten worden zijn: wanneer willen we datagedreven werken, en wanneer mag het ook datagestuurd? Wanneer willen we een algoritme impact assessment, waarbij we algoritmen eventueel ook aan genoemde toezichtscommissie voorleggen?
- Zo'n afweging is een politieke keuze, en het is daarom van belang deze afweging bij raadsleden en statenleden te leggen, liefst na consultatie van de (enkele) technologisch geschoolde burger.

De consequentie van bijvoorbeeld dataminimalisatie en het niet gebruiken van oncontroleerbare algoritmen, is wel dat er soms maatschappelijke kansen onbenut zullen blijven. Transparantie en 'de menselijke maat' zullen dan boven efficiëntie en/of effectiviteit gaan. Het is aan gemeenteraden en Provinciale Staten om over deze gemiste kansen verantwoording af te leggen aan de burger

Borging in de organisatie

Het is dus mijns inziens vooral aan overheden zelf om meer sturing en richting te geven aan een integere omgang met nieuwe technologieën. Als overheden zelf aan de slag moeten, betekent dit uiteraard ook dat politici, bestuurders en ambtenaren de benodigde technologisch, juridische en ethische kennis in huis moeten hebben of aan moeten weten te boren.

Juist bestuurders en raads- en statenleden zullen zich dan moeten ontwikkelen tot 'technologisch bestuurder / volksvertegenwoordiger'. Het begint natuurlijk bij besef van de problematiek. Een lokaal, regionaal en/of nationaal debat om de publieke waarden in relatie tot digitalisering te doorleven, lijkt me dan ook uitermate zinvol. Het Amsterdamse manifest Tada kan een aanzet geven tot zo'n debat, maar zou niet domweg 'overgenomen' moeten worden. Het is juist van belang dat alle betrokkenen gezamenlijk tot eigen conclusies komen.

In de meeste ambtelijke organisaties is nu nog niet voldoende technologische en ethische kennis aanwezig om goed vorm te geven aan een integere omgang met de digitalisering van overheidstaken. In beleidsafdelingen zal een zekere basiskennis van de materie nodig zijn, juist om te weten wanneer men hulp moet inroepen van specialisten. Dit zal in interne opleidingstrajecten geborgd moeten worden.

Wat betreft interne specialistische ondersteuning, is het belangrijk te beseffen dat de vereiste deskundigheid vaak niet aanwezig zal zijn bij de ICT-afdelingen. Deze houden zich immers vooral bezig met het draaiend houden van de reguliere ICT-systemen, hetgeen andere competenties vraagt dan nodig zijn om datavergaring, datadeling en dataverwerking vanuit ethisch perspectief te beoordelen. Gezien het feit dat data werkelijk overal en altijd in de organisatie, zowel bij beleid als bij uitvoering, een belangrijke rol (zullen) spelen, kan de benodigde deskundigheid niet voortdurend extern ingehuurd worden. Het is dan handig om de eventueel al aanwezige kennis van data, ethiek en dergelijke zoveel mogelijk te bundelen en indien nodig aan te vullen met extra deskundigheid of deskundige capaciteit. Denk bij bundeling van bestaande capaciteit bijvoorbeeld aan de func-

tionaris gegevensbescherming en de integriteitscoördinator die veel overheidsorganisaties al in huis hebben.

Verder is het natuurlijk van belang dat overheden hun ethische principes ook als uitgangspunt nemen ingeval de private sector betrokken wordt bij de taakuitvoering van de overheid. Hierbij is het door het Rathenau Instituut voorgestelde nationale 'digitaliseringsakkoord' zinvol om de private sector bewust te maken van het feit dat de overheid wellicht extra zware eisen stelt aan te leveren producten en diensten (Kool e.a. 2017, p. 14-15). Deze dialoog wordt naar verwachting concreter – en daarmee zinvoller - als er overeenstemming is tussen overheden over wat die eisen dan zouden moeten zijn.

Overzicht van gebruikte bronnen

- Algemene Rekenkamer (2016). Aanpak van laaggeletterdheid. Den Haag: Algemene Rekenkamer. Opgeroepen op 22 september 2018 van https://www.rekenkamer.nl/publicaties/rapporten/2016/04/20/aanpak-van-laaggeletterdheid
- Amsterdam Economic Board (2017). Tada. Duidelijk over data. Opgeroepen op 5-6-2018 van https://tada.city/
- Berinato, S. (2018). Stop thinking about consent it isn't possible and it isn't right. Harvard Business Review, 24-9-2018. Opgeroepen op 4 oktober 2018 van https://hbr.org/2018/09/stop-thinking-about-consent-it-isnt-possible-and-it-isnt-right
- Borghuis, D. (2018). Wifi-tracking Enschede. Opgeroepen op 11 augustus 2018 van daveborghuis.nl: http://daveborghuis.nl/wp/wifi-tracking/
- Brazilian Civil Rights Framework for the Internet. Opgeroepen op 7 september 2018 van Wikipedia: https://en.wikipedia.org/wiki/Brazilian_Civil_Rights_Framework_for_the_Internet
- Bulut-Keskin, Ö. (2018, 8). VNG-Handreiking: Wet hergebruik overheidsinformatie. VNG. Opgeroepen van https://vng.nl/onderwerpenindex/dienstverlening-en-informatiebeleid/dienstverlening-aan-inwoners-en-ondernemers/nieuws/wet-hergebruik-overheidsinformatie-vng-handreiking.
- Coalitieakkoord Amsterdam (2018, 5). Een nieuwe lente een nieuw geluid. Coalitieakkoord Groen Links/D66/PVDA/SP - Mei 2018, p.58-59. Opgeroepen op 7 september 2018 van www.Amsterdam.nl: https://www.amsterdam.nl/bestuur-organisatie/volg-beleid/coalitieakkoord-2018/
- ContentWorks IDG (2018, 5 29). Wat als een zelflerend algoritme niet te controleren is? Opgeroepen van CIO.nl: https://cio.nl/big-data/105063-wat-als-een-zelflerend-algoritme-niet-te-controleren-is
- Dubbeld, L. (2017). Predictive policing: Niet alleen een zaak van de politie. Security Management, september 2017. Opgeroepen op 4 augustus 2018 van https://www.google.com/search?q=Dubbeld.+L%2C+%E2%80%9CPredictive+policing%3A+Niet+alleen+een+zaak+van+-de+politie%E2%80%9D.+Security+Management.+Sept+2017
- Elibol, R. (2018). Transparantie, ook als het niet uitkomt. De Groene Amsterdammer 2 mei 2018. Opgeroepen op 4 september 2018 van www.groene.nl: https://www.groene.nl/artikel/transparantie-ook-als-het-niet-uitkomt
- Europese Commissie (2014). EU Innovation and Networks Executive Agency, Horizon 2020 Programma, Smart Cities & Communities. Funding areas. Opgeroepen op 15 september 2018 van ec.europa.eu: https://ec.europa.eu/inea/en/horizon-2020
- Europese Commissie (2018). Next Generation Internet Initiative. Opgeroepen op 9 november 2018 van https://ec.europa.eu/digital-single-market/en/next-generation-internet-initiative
- Gartner (z.d.). IT Glossary. Opgeroepen op 4 augustus 2018 van www.gartner.com: https://www.gartner.com/it-glossary/big-data/
- Gemeente Nijmegen (2018). Gemeente Nijmegen werkt mee aan pilot 'digitale identiteit' met app IRMA. Opgeroepen op 26 september 2018 van www.nijmegen.nl: https://www.nijmegen.nl/nieuws/app-irma/
- Geonovum (2017). Aan de slag met sensordata. Spelregels voor data ingewonnen in de openbare ruimte. Geonovum. Opgeroepen op 11september 2018 van Geonovum.nl: https://www.geonovum.nl/over-geonovum/actueel/spelregels-voor-sensoren-in-openbare-ruimte
- Hardesty, L. (2015). Identity Privacy challenges. Analysis: It's surprisingly easy to identify individuals from credit-card metadata. MIT News, 29-1-2015,
- Opgeroepen op 2 oktober 2018 van http://news.mit.edu/2015/identify-from-credit-card-metadata-0129
- Hartholt, S. (2017). Depressies voorspellen met data. Binnenlands Bestuur, 13 januari 2017. Opgeroepen op 4 augustus 2018 van www.binnenlandsbestuur.nl: https://www.binnenlandsbestuur.nl/digitaal/nieuws/depressies-voorspellen-met-data.9555894.lynkx
- Hartholt, S. (2018). D66 wil 'algoritme-waakhond'. Binnenlands Bestuur, 25 september 2018. Opgeroepen op 30 september 2018 van www.binnenlandsbestuur.nl: https://www.binnenlandsbestuur.

nl/digitaal/nieuws/d66-wil-algoritme-waakhond.9597736.lynkx
- Hempel, J. (2018). Want to Prove Your Business Is Fair? Audit Your Algorithm. Wired. Opgeroepen op 11 oktober 2018 van Wired.com: https://www.wired.com/story/want-to-prove-your-business-is-fair-audit-your-algorithm/
- Issa, D. (2012). A Digital Citizen's Bill of Rights. Opgeroepen op 7 september 2018 van Keepthewebopen.com: http://keepthewebopen.com/digital-bill-of-rights
- Kamerbrief over motie over transparantie van algoritmen in gebruik bij de overheid (2018). Opgeroepen op 19 oktober 2018 van www.rijksoverheid.nl: https://www.rijksoverheid.nl/documenten/kamerstukken/2018/10/09/tk-transparantie-van-algoritmes-in-gebruik-bij-de-overheid
- Kamerstuk 32761 nr. 118. (2018). Opgeroepen van www.overheid.nl: https://zoek.officielebekendmakingen.nl/kst-32761-118.html
- Kleinnijenhuis, J. (2018). Belastingdienst: het is 'technisch onmogelijk' persoonsgegevens goed te beveiligen. Trouw 12 oktober 2018. Opgeroepen op 1 oktober 2018 van www.trouw.nl: https://www.trouw.nl/home/belastingdienst-het-is-technisch-onmogelijk-persoonsgegevens-goed-te-beveiligen~a8648a26/
- Kool, L. J., Timmer J., Royakkers L. & Van Est, R. (2017). Opwaarderen. Borgen van publieke waarden in de digitale samenleving. Den Haag: Rathenau Instituut. Opgeroepen van www.rathenau.nl: https://www.rathenau.nl/nl/digitale-samenleving/opwaarderen
- Kuiken, A. (2010). "WOB-expert bepleit Autoriteit Openbaarheid". Trouw 29 september 2010. Opgeroepen van www.trouw.nl: https://www.trouw.nl/home/wob-expert-bepleit-autoriteit-openbaarheid~a036e692/
- Kuipers, R., Van der Steenhoven, K. & Staal, J. (2016). Quick scan impact Wet open overheid (Woo). Opgeroepen op 4 augustus 2018 van www.rijksoverheid.nl: https://www.rijksoverheid.nl/documenten/rapporten/2016/12/13/quick-scan-impact-wet-open-overheid-woo
- Kuipers, R., Van der Steenhoven, K. & Staal, J. (2017). Quick scan impact Wet open overheid (Woo), deel 2. Opgeroepen op 4 augustus 2018 van www.rijksoverheid.nl: https://www.rijksoverheid.nl/documenten/rapporten/2017/05/30/quick-scan-impact-wet-open-overheid-woo-deel-2
- Masterclass Frans Feldberg bij Provincie Noord-Holland, Haarlem 2 oktober 2018.
- Masterclass Monica Wigman bij Provincie Noord-Holland. Haarlem 28 juni 2018.
- Meijer, E. & Schouten, S. (2017). Politieke agenda voor technologie ontbreekt. De Helling nr 4. Opgeroepen op 10 september 2018 van waag.org: https://waag.org/nl/article/politieke-agenda-voor-technologie-ontbreekt
- Ministerie van Binnenlandse Zaken (2009). Code goed openbaar bestuur. Opgeroepen op 15 september 2018 van Rijksoverheid.nl: https://www.rijksoverheid.nl/onderwerpen/kwaliteit-en-integriteit-overheidsinstanties/gedragscode-openbaar-bestuur
- Ministerie van Infrastructuur en Milieu (2017). Nationale Markt- en Capaciteitsanalyse. Opgeroepen op 5 augustus 2018 van www.rijksoverheid.nl : https://www.rijksoverheid.nl/documenten/rapporten/2017/05/01/nationale-markt-en-capaciteitsanalyse-2017-nmca
- Tweede Kamer der Staten Generaal (2018). Mondelinge vragen van het lid Raemakers (D66) aan de Staatssecretaris van Sociale Zaken en Werkgelegenheid over het bericht «Algoritme voorspelt wie fraude pleegt bij bijstandsuitkering» (Nrc.nl, 8 april 2018) (ingezonden 10 april 2018). (2018). Tweede Kamer, vergaderjaar 2017–2018, Vragen. Opgeroepen van overheid.nl: https://zoek.officielebekendmakingen.nl/kv-tk-2018Z06578.html
- Naafs, S. (2017, 12 6). De muren hebben sensoren: Smart cities, de stad als datamijn. De Groene Amsterdammer no 49. Opgeroepen op 12 augustus 2018 van https://www.groene.nl/artikel/de-muren-hebben-sensoren
- NCJ. (2018). Techagenda in de praktijk. Opgeroepen op 10 september 2018 van Nederlands Centrum Jeugdgezondheid: https://www.ncj.nl/techagenda-in-de-praktijk/
- NOS (2016). "Deze Nederlandse student reconstrueerde gesprekken Turkse coupplegers." (26 juli 2016). Opgeroepen op 2 oktober 2018 van NOS.nl: https://nos.nl/op3/artikel/2120996-deze-nederlandse-student-reconstrueerde-gesprekken-turkse-coupplegers.html

- O'Neil, C. (2017). Weapons of Mass Destruction. How Big Data Increases Inequality and Threatens Democracy. Penguin Books Ltd.
- Praktijkproef Amsterdam (2017). Opgehaald van https://www.praktijkproefamsterdam.nl/
- Provincie Noord-Holland (2018a). Communicerende auto's getest op eerste slimme weg. Opgeroepen op 10 september 2018 van www.noord-Holland.nl: https://www.noord-holland.nl/Actueel/Archief/2018/September_2018/Communicerende_auto_s_getest_op_eerste_slimme_weg
- Provincie Noord-Holland (2018b). Datastrategie van de Provincie Noord-Holland: Aanzet voor innovatief en verbindend data-gedreven werken. Opgeroepen op 30 september 2018 van https://api1.ibabs.eu/publicdownload.aspx?site=noordholland&id=1100076048
- Purtova, N. (2018). The law of everything. Broad concept of personal data and future of EU data protection law. Journal of Law, Innovation and Technology, 40-81. Opgeroepen op 2 oktober 2018 van https://www.tandfonline.com/doi/full/10.1080/17579961.2018.1452176
- Raad van State (2012). Advies W04.12.0249/I. Kamerstukken II 2013/14, 33 328, nr. 7. Opgeroepen op 11 augustus 2018 van https://www.raadvanstate.nl/adviezen/zoeken-in-adviezen/tekst-advies.html?id=10540
- Raad van State (2018). Advies W04.18.0230/I. Kamerstukken II 2017/18, 26643, nr. 557. Opgeroepen op 7 september 2018 van https://www.raadvanstate.nl/adviezen/zoeken-in-adviezen/tekst-advies.html?id=13065
- Reisman, D. J., Schulz, J., Crawford, K. & Whittaker, M. (2018a). Agencies should conduct a self-assessment of existing and proposed automated decision systems, evaluating potential impacts on fairness, justice, bias, or other concerns across affected communities. Opgeroepen op 2 oktober 2018 van medium.com/@AINowInstitute: https://ainowinstitute.org/aiareport2018.pdf
- Reisman, D. J., Schulz, J., Crawford, K. & Whittaker, M. (2018b). Algorithmic Impact Assessments: Toward Accountable Automation in Public Agencies. Opgeroepen op 15 augustus 2018 van medium.com/@AINowInstitute: tps://medium.com/@AINowInstitute/algorithmic-impact-assessments-toward-accountable-automation-in-public-agencies-bd9856e6fdde
- Rijksoverheid (2018). Mobility as a Service – regionale pilots. Opgeroepen op 15 augustus 2018 van www.rijksoverheid.nl: https://www.rijksoverheid.nl/documenten/brochures/2018/06/25/mobilty-as-a-service---regionale-pilots
- Rijkswaterstaat (z.d.). Augmented reality en Rijkswaterstaat. Hoe zien we de snelweg in de toekomst? Opgeroepen op 4 november 201, van www.rijkswaterstaat.nl: https://www.rijkswaterstaat.nl/rws/AugumentedReality/voorbeelden-rijtaakondersteuning.php
- Van Est, R., De Bakker, E., Van den Broek, J., Deuten, J., Diederen, P., Van Keulen, I., Korthagen, I. & Voncken, H. (2018). Waardevol digitaliseren – Hoe lokale bestuurders vanuit publiek perspectief mee kunnen doen aan het 'technologiespel'. Den Haag: Rathenau Instituut. Opgeroepen op 31 augustus 2018 van www.rathenau.nl: https://www.rathenau.nl/nl/digitale-samenleving/waardevol-digitaliseren
- Safi, M. (2018, 9 26). Indian court upholds legality of world's largest biometric database. The Guardian, 26-9-2018. Opgeroepen op 26 september 2018, van www.theguardian.com: https://www.theguardian.com/world/2018/sep/26/indian-court-upholds-legality-of-worlds-largest-biometric-database
- Schuurmans, U. (2018, 10 16). Voorspellende geneeskunde. ICT & Health. Opgeroepen op 18 oktober 2018, van www.icthealth.nl: https://www.icthealth.nl/blog/voorspellende-geneeskunde/
- Smith, A. (2018). Franken-algorithms: the deadly consequences of unpredictable code. The Guardian 30-8-2018. Opgeroepen op 30 augustus 2018 van www.theguardian.com: https://www.theguardian.com/technology/2018/aug/29/coding-algorithms-frankenalgos-program-danger
- Thaler, R. &. Sunstein, C. (2018). Nudge. Naar betere beslissingen over gezondheid, geluk en welvaart (8e druk). (C. Zijlemaker, Vert.) Amsterdam/Antwerpen: Uitgeverij Business Contact.
- The Digital Republic Bill - Overview (2014). Opgeroepen op 9 juli 2018 van La République Numérique: https://www.republique-numerique.fr/pages/in-english
- Van der Wel, E. (2015). Algoritmes beslis-

sen steeds meer voor ons, maar we weten niet hoe ze dat doen. Opgeroepen van Numrush.nl: http://numrush.nl/2015/11/16/algoritmes-beslissen-steeds-meer-voor-ons-maar-we-weten-niet-hoe-ze-dat-doen/
- Van Zon, H. (2018). Wat vindt de Eerste Kamer? Ibestuur Online. Opgeroepen op 14 augustus 2018 van ibestuur.nl: https://ibestuur.nl/weblog/de-woo-wat-vindt-de-eerste-kamer
- Waag Technology and Society (2018). DECODE. Opgeroepen op 2 oktober 2018 van Waag.org: https:// DECODEproject.eu/
- Weijts, C. (2018, 11 2). Tandenborstels tellen 2.0. NRC 2-11-2018. Opgeroepen op 2 november 2018 van https://www.nrc.nl/nieuws/2018/11/02/tandenborstels-tellen-20-a2753672
- Wetenschappelijk Onderzoek en Documentatiecentrum (2011). Function creep en privacy. Justitiële Verkenningen. nr. 8, 6. Opgeroepen op 22 oktober 2018 van www.wodc.nl: https://www.wodc.nl/onderzoeksdatabase/jv201108-function-creep-en-privacy.aspx
- Wetenschappelijke Raad voor Regeringsbeleid (2017). Weten is nog geen doen. Een realistisch perspectief op redzaamheid. Opgeroepen op 22 september 2018 van www.wrr.nl: www.wrr.nl/publicaties/rapporten/2017/04/24/weten-is-nog-geen-doen.
- Wielaard, N. (2018). Cathy O'Neill heeft primeur van eerste algoritme. Opgeroepen van www.accountant.nl: https://www.accountant.nl/artikelen/2018/7/cathy-oneill-heeft-primeur-van-eerste-algoritme-audit/