Slaaf van het algoritme

Lanzing, M.

Publication date
2018
Document Version
Final published version
Published in
Wijsgerig Perspectief

Slaaf van het algoritme

Wat betekenen slimme algoritmes die ons gedrag kunnen sturen voor onze privacy en autonomie? **MARJOLEIN LANZING** gaat in op de gevaren van algoritmes die ons gedrag beïnvloeden op basis van big data, en onderzoekt hoe deze beïnvloeding zich verhoudt tot onze democratie.

Onze online omgeving wordt steeds meer op ons afgestemd. Met elke minuut die we doorbrengen op onze smartphones, tablets en computers weet onze digitale omgeving meer over ons. Steeds meer technologieën gebruiken deze 'kennis' om in te spelen op ons gedrag en op onze voorkeuren. Het 'realtime' verzamelen van data om gebruikers aanbevelingen te doen en hen te sturen in hun keuzes en gedrag is een van de meest veelbelovende ontwikkelingen op technologiegebied. Van hun kant vinden gebruikers het maar wat aantrekkelijk dat hun Uber-app realtime informatie verzamelt om hun volgende rit te voorspellen, en hen tijdens het ritje een sushi-restaurant aanbeveelt op basis van hun persoonlijke voorkeur. Dat digitaal warenhuis Amazon jouw informatie verzamelt om je gepersonaliseerde aanbiedingen te doen en zelfs kan voorspellen wanneer je toe bent aan je volgende roman van Knausgard vindt menigeen handig. En dat FitBit gebruikmaakt van gepersonaliseerde *nudges* om gebruikers van hun fitness-apps en apparaatjes gezondere keuzes te laten maken, is voor velen juist een reden om er op 1 januari een aan te schaffen.

Tegelijkertijd worden nieuwe technologieën die onze data gebruiken om ons gedrag te sturen met argusogen bekeken. En terecht, want de angst voor (massa-)manipulatie is verre van paranoïde. Het kwam Facebook al in 2014 op kritiek te staan: het bedrijf kwam toen in het nieuws vanwege het 'Facebook Experiment', waarin het de tijdlijnen van gebruikers aanpaste om hun gedrag te beïnvloeden. Momenteel is Facebook wederom in het nieuws: de data van miljoenen Facebookgebruikers zijn door datamining-bedrijf Cambridge Analytica gebruikt om het stemgedrag van Amerikaanse burgers te beïnvloeden met behulp van gepersonaliseerde politieke advertenties en artikelen, waaronder volgens klokkenluider Christopher Wylie nepnieuws, zodat ze op de Republikeinse kandidaat Donald Trump zouden stemmen. Toen er data werden verzameld en algoritmes 'gewoon' werden ingezet voor het aanraden van een film, boek of Facebookvriend, kraaide er in *the land of the free* geen haan naar de geniale techondernemer Mark Zuckerberg. Nu blijkt dat er gemorreld kan worden aan de waardevolle

democratische procedure moet hij bij de Amerikaanse Senaat voorkomen — al werd hij tijdens de eerste dag van zijn verhoor alsnog herhaaldelijk gecomplimenteerd met het waarmaken van de American Dream.

De affaire Facebook-Cambridge Analytica heeft een publieke discussie op gang gebracht over de manipulatieve kanten van *hypernudges*. Hypernudges zijn gepersonaliseerde aanbevelingen. Ze worden gegenereerd door slimme algoritmes op basis van big data en hebben je gedrag beïnvloeden als doel. Ze maken deel uit van de bredere trend richting een 'algocratie': een samenleving waarin steeds meer aspecten van ons leven en van onze maatschappij gereguleerd worden door algoritmes die op basis van big data beslissingen nemen. Daarmee gaat de discussie nu vooral over de macht van de giganten achter deze technologieën die hier geld aan verdienen. De zogenaamde *Frightful Five*: Facebook, Google, Apple, Microsoft en Amazon.

Deze vijf megabedrijven handelen in data, de digitale olie, en hebben in het neoliberale klimaat van de Verenigde Staten alle ruimte gekregen om zich zonder al te veel overheidsinmenging te ontwikkelen tot dominante actoren met een enorme machtspositie op de datamarkt. Shoshana Zuboff, hoogleraar Business aan Harvard, spreekt zelfs van een transformatie van het kapitalisme binnen de informatiesamenleving. Het 'surveillance-kapitalisme' draait om het vermarkten van data die worden gewonnen door surveillance. De nieuwe markten die volgens haar binnen het surveillance-kapitalisme worden aangeboord zijn die van gedragsvoorspelling en gedragsbeïnvloeding.

In dit essay werp ik enkele kritische vragen op met betrekking tot het gebruik van hypernudges door grote commerciële tech-bedrijven, vanuit een privacy-filosofisch perspectief. Wat betekenen slimme algoritmes die ons gedrag kunnen sturen op basis van big data voor onze privacy en autonomie? En, sociaal-politiek gezien: hoe verhoudt de inzet van hypernudges, zoals gebruikt door Facebook en Cambridge Analytica, zich tot de democratie?

DUWTJE IN DE RUG

Veel nieuwe technologieën beloven de autonomie van gebruikers te versterken via gepersonaliseerde feedback op basis van big data. Zo wordt gebruikers een persoonlijke route aangeboden in de *information overload* van producten, diensten en informatie die ze dagelijks te verduren krijgen (Van den Berg 2016). Ook kunnen gepersonaliseerde aanbevelingen op basis van 'objectieve' data nuttige inzichten opleveren en gebruikt worden om eindelijk eens je hardloopschoenen aan te trekken. *Self-trackers*, bijvoorbeeld, kunnen zich op basis van data vergelijken met anderen en de controle over hun gezondheid en fitness (terug)winnen met behulp van handige aanbevelingen die inspelen op hun dataprofiel. Gepersonaliseerde feedback kan een manier zijn om gebruikers te ondersteunen in een autonoom leven. Technologie kan gebruikers helpen om de keuzes te maken die ze *willen* maken. Een soort duwtje in de rug.

'Technologie kan gebruikers helpen om de keuzes te maken die ze *willen* maken'

Zo'n duwtje noemen we ook wel een 'nudge'. De nudge werd in 2008 razend populair dankzij het gelijknamige boek van Richard Thaler en Cass Sunstein. Een nudge is een ingreep in de omgeving, een bepaalde 'keuzearchitectuur', die het gedrag van mensen op voorspelbare wijze verandert, zonder andere opties weg te nemen of bijvoorbeeld onaantrekkelijk te maken met behulp van een financiële prikkel. Nudges compromitteren in theorie je vrijheid niet. Thaler en Sunstein noemen nudges 'libertair paternalistisch'. Het libertair paternalisme houdt in dat je de keuze van mensen zo kan sturen dat ze uiteindelijk kiezen wat het beste is voor henzelf als ze niet waren beperkt door menselijke tekortkomingen zoals wilszwakte. Dat riekt naar louter paternalisme, ware het niet dat mensen *in theorie* nog steeds vrij zijn om te kiezen. Nudges nemen geen opties weg, maar rangschikken opties op zo'n manier dat bepaalde varianten beter overkomen. Een voorbeeld is een op de grond getekende rode pijl die naar de trap wijst om mensen te laten traplopen in plaats van de lift te laten nemen. Volgens sommigen versterken nudges dus juist de autonomie van mensen omdat ze uiteindelijk, op basis van een minimale ingreep, mensen ondersteunen om te kiezen wat ze *willen* kiezen. Libertair paternalisme is geen oxymoron, geen paradox, zeggen Thaler en Sunstein dan ook. Goede vondst, want zonder dat geruststellende dekentje van libertarisme was de nudge nooit populair geworden in de Verenigde Staten.

Desalniettemin laat niet iedereen zich inpakken. De kritiek op nudgen is dat het manipulatief is (Hausman en Welch 2010). In plaats van mensen aan te spreken op hun rationele capaciteiten worden zij gestuurd door verborgen systemen die inspelen op onderbewuste, psychologische mechanismen (Nys en Engelen 2016). Ze zijn op dat moment dus niet de baas over hun gedrag.

Om deze kritiek te ondervangen bedacht Thaler drie criteria. Zo moeten goede nudges en hun makers zichtbaar en aansprakelijk zijn en nooit misleidend.Daarbij moet het altijd makkelijk zijn om niet mee te doen aan een nudge, de zogenaamde 'opt-out'. Tot slot moet het zo zijn dat een nudge altijd het welzijn van de 'nudgee' voor ogen heeft (Thaler 2015).

Laten we voor het gemak aannemen dat we nudges kunnen accepteren mits ze aan Thalers criteria voldoen. Geldt dat voor nudges in de online omgeving, die worden aangedreven door big data?

ONZICHTBAAR

Nudges die worden gevoed met big data noemen we 'hypernudges'. Hypernudges zijn algoritmisch gepersonaliseerde online keuze-architecturen (Yeung 2017). Met keuze-architectuur bedoel ik de (rangschikking van) opties die je in de online omgeving worden aanbevolen. Welke opties dat zijn en in welke volgorde wordt constant realtime door deze algoritmes aangepast op basis van enorme hoeveelheden data. Hierbij moet je denken aan de gepersonaliseerde reclames en artikelen die Facebook je aanbeveelt op basis van jouw surfgedrag en dat van 'anderen zoals jij' die vergelijkbare politieke, muziek- of lifestyle- interesses hebben. Of denk aan Google Maps, die zodra jij je route wijzigt of wanneer er een file ontstaat, jou een op maat gemaakte route aanbeveelt op basis van je nieuwe gps- informatie en de informatie van andere Google Maps-gebruikers.

Hypernudges claimen door verschillende databronnen aan te boren uiteindelijk 'voorspellingen' te kunnen doen over de interesses, gewoonten en voorkeuren van de personen waar zij zich op richten, en hun keuzes te kunnen sturen. Hypernudges zijn veel geraffineerder, krachtiger en bemoeizuchtiger dan gewone nudges. Hypernudges zijn dynamisch. Ze verschaffen realtime gepersonaliseerde feedback en opties. Dat wordt mogelijk gemaakt door constante data-verzameling, oftewel surveillance door commerciële partijen. Op basis van de data wordt het mogelijk om de keuze-architecturen van miljoenen gebruikers met een muisklik te veranderen en ze allemaal een gepersonaliseerde set opties aan te bieden. Een gewone nudge richt zich daarentegen op een algemeen publiek en biedt alleen een *one size fits all*-optie.

Daarbij hebben hypernudges een 'voorspellende' kracht. Slimme algoritmes kunnen 'leren' van de data, gedragsvoorspellingen doen en daarop de keuzes van gebruikers aanpassen. Gewone nudges zijn traag, omdat ze niet beschikken over adequate feedback of de mogelijkheid om hun interventies meteen aan te passen om ze effectiever te maken.

Tot slot zijn hypernudges onzichtbaar geïntegreerd in de structuur van jouw online omgeving. Je kunt ze dus niet zien. Dit maakt het ook heel ingewikkeld om de intenties achter hypernudges te zien. Het is vaak niet duidelijk dat de architecten achter hypernudges commerciële partijen zijn die economische redenen hebben om gebruikers te sturen in hun gedrag. Gewone nudges zijn misschien ook niet opvallend, maar ze zijn wel zichtbaar in de fysieke wereld. We kunnen de rode pijl richting de trap zien, en er dus ook vragen over stellen.

Al deze eigenschappen maken dat hypernudges niet aan Thalers criteria voldoen. Hypernudges zijn niet transparant en het is lastig te achterhalen of het welzijn van de gebruiker voorop staat wanneer er commerciële partijen achter zitten. Verder is het lastig om 'nee' te zeggen tegen en te ontsnappen aan een hypernudge die je niet kunt zien.

Het feit dat hypernudges niet voldoen aan deze criteria maakt het zeer waarschijnlijk dat ze manipulatief zijn en dus een bedreiging voor de autonomie, in plaats van een versterking ervan. Bovendien, als we verder inzoomen op de eigenschappen van hypernudges zien we dat er ook een substantiële reden is waarom ze onze autonomie bedreigen.

BEDREIGDE AUTONOMIE

Voor het leiden van een autonoom leven en voor een diversiteit en pluraliteit van zelfgekozen leefstijlen, gedrag, acties en keuzes (natuurlijk zonder te claimen dat deze geïsoleerd van een sociale omgeving tot stand komen) hebben we privacy nodig. Privacy en autonomie verhouden zich via een functionele relatie tot elkaar. De reden waarom we privacy waardevol vinden, is omdat het geworteld is in autonomie. Maar tegelijkertijd kunnen we privacy niet tot autonomie of welke andere waarde dan ook reduceren (Roessler 2005). Privacy is een sociale onderhandeling en houdt grofweg in dat iemand min of meer in de hand heeft wie er toegang heeft tot zijn of haar persoonlijke informatie en beslissingen, en in hoeverre. Redelijke verwachtingen op basis van wetten en sociale normen spelen hier een belangrijke rol in. We kunnen er bijvoorbeeld redelijkerwijs van uitgaan dat informatie die we delen met onze dokter niet bij een zorgverzekeraar belandt. Of bij de staat. Of bij je werkgever.

Op eenzelfde manier houdt privacy ook in dat je enigszins in de hand hebt wie zich mag

bemoeien met je beslissingen en acties. Met 'bemoeien' bedoel ik welke actoren of entiteiten jouw beslissingen en acties mogen becommentariëren, interpreteren of sturen. Wat geldt als ongewenste of gewenste inmenging is natuurlijk een dynamische, sociale onderhandeling die per sociale context verschilt: je partner mag zich wel met de opvoeding van de kinderen bemoeien, maar van commentaar door onze werkgever zouden we vreemd opkijken. In het geval van hypernudging zouden we bijvoorbeeld de redelijke verwachting moeten kunnen hebben dat onze Facebookdata niet gebruikt worden door overheden of commerciële bedrijven om ons te sturen in onze politieke voorkeuren en ons stemgedrag.Maar door big data gedreven technologieën, zoals hypernudges, vervagen langzaam de grenzen tussen deze contexten. Traditionele middelen om accurate verwachtingen te scheppen rondom het delen en verzamelen van informatie, zoals transparantie en geïnformeerde toestemming, staan onder druk en zijn moeilijk te handhaven. Nieuwe technologieën maken het mogelijk voor partijen om toegang te krijgen tot contexten waar gebruikers hen voorheen geen toestemming voor gaven, of hen niet verwachtten. Facebook, Amazon en Google weten wanneer gebruikers proberen te stoppen met roken, wanneer ze gewicht willen verliezen, wanneer ze op een Democraat willen stemmen, wanneer ze een gezin willen stichten of van carrière willen veranderen. Die informatie deelden we voorheen alleen met onze arts, het stemhokje of onze partner. Bovendien weten ze op basis van deze informatie welke beslissingen we zeer waarschijnlijk zullen maken in de toekomst. Beslissingen die we liever bespreken en laten beïnvloeden door onze arts, een politiek debat, of onze partner — niet door een bedrijf.

'Facebook, Amazon en Google weten wanneer gebruikers proberen te stoppen met roken'

Het schandaal rondom Facebook en Cambridge Analytica is problematisch vanuit een privacy-perspectief. Ten eerste vanwege de ongeëvenaarde schaal van dataverzameling via doorlopende surveillance. Ten tweede omdat de surveillance en de algoritmes die Facebook gebruikt om je te sturen in je gedrag onzichtbaar zijn. Wat dit problematisch maakt, is dat deze praktijken worden uitgevoerd door een commerciële keuze-architect met economische motieven, die zich bemoeit met een domein waarin we normaal gesproken geen commerciële bemoeienis verwachten of willen: de politiek. Commerciële hypernudges schenden de privacy en maken gebruikers daarmee kwetsbaar voor manipulatie. Een schending van de privacy is een bedreiging voor de autonomie van gebruikers.

KWETSBAARHEID

Met de opkomst van het 'surveillance-kapitalisme' raken we steeds meer de controle over onze informatie en beslissingen — onze privacy — kwijt en worden we steeds kwetsbaarder voor manipulatie. Veel gebruikers weten niet hoe hun data nu al gebruikt worden, laat staan in de toekomst (Mittelstadt en Floridi 2016). Gebruikers 'betalen' met hun data voor de diensten van een commercieel bedrijf, dat ze dan weer gebruikt voor eigen commerciële doeleinden.

ESSAY

Data die nu worden verzameld, kunnen straks gebruikt worden om voorspellingen te doen over hoe gebruikers zich zullen gedragen in de toekomst. Data kunnen met terugwerkende kracht gebruikt worden voor doelen die onze huidige verbeeldingskracht overstijgen. Je hiervan bewust zijn kan een *chilling effect* teweegbrengen: je gaat je gedrag aanpassen aan een vermeende sociale norm uit angst voor (sociale) sancties. Dit gebeurde bijvoorbeeld in de Verenigde Staten nadat Edward Snowden bekend had gemaakt dat de National Security Agency op grote schaal data had verzameld over Amerikaanse burgers. Gebruikers pasten hun zoekgedrag op Google aan.

Verder liggen er uitsluiting en discriminatie op de loer. Om gebruikers preciezer en lucratiever te kunnen 'targeten', construeren tech-bedrijven profielen: stereotiepe, sociale categorisaties van datapatronen. Profielen zorgen voor nieuwe vormen van kwetsbaarheid. Ze verbergen sociale contexten en relaties door gedrag te reduceren tot data: data die je gemakkelijk kunt manipuleren en die gehuld gaan in een aura van objectiviteit en neutraliteit. Een recent voorbeeld is het onderzoek van Investico naar creditscoring in Nederland. Als je in een bepaalde wijk woont waar de postcode correspondeert met 'wanbetaling', kan je uitgesloten worden van bepaalde diensten zoals abonnementen en leningen (zie ook O'Neil 2016; Pasquale 2015). Andere voorbeelden zijn dat vrouwen op Google lange tijd minder vacatures voor goedbetaalde banen te zien kregen dan mannen en dat Afro-Amerikaanse namen in de Google-zoekfunctie geassocieerd worden met criminaliteit. Wat het voorgaande nog verder compliceert, is dat een deel van de slimme algoritmes achter deze categorisaties *black boxes* zijn: ze zijn zo complex dat zelfs de makers niet altijd begrijpen waarom ze een bepaalde output opleveren, laat staan dat gebruikers dit kunnen corrigeren (Pasquale 2015).

'Bij het verzamelen van data ligt uitsluiting en discriminatie op de loer'

Gebruikers kunnen met behulp van hypernudges gestuurd worden in een bepaalde commerciële of politieke richting. Dat is een lucratieve business. Wat je te zien krijgt op platforms als Facebook wordt bepaald door wie daarvoor betaalt. Daarmee is de nudge zijn geruststellende dekentje van libertarisme kwijtgeraakt in de big data-storm. Als je door een slim algoritme van elke honderd posts er maar tien te zien krijgt, dan worden er opties weggenomen. Hier komen ook de bezwaren vandaan rondom de filterbubbel, de tunnelvisie die ontstaat op basis van een gepersonaliseerde online omgeving. Het is ingewikkeld om erachter te komen welke opties er niet zichtbaar zijn en om te onderhandelen over wat je standaard wordt aanbevolen (Brey 2016). Bovendien: bij wie zou je dit moeten aankaarten? Deze systemen hebben geen onmiddellijk zichtbare verantwoordelijke die aansprakelijk kan worden gehouden. Facebook bood pas heel recentelijk zijn excuses aan voor de al sinds 2016 voortslepende nepnieuwsaffaire, omdat het bedrijf zich in eerste instantie werkelijk niet verantwoordelijk *voelde* voor wat er was gebeurd.

VOORSPELBAAR OBJECT

Tech-giganten als Facebook schenden onze privacy omdat ze op ongekende schaal data verzamelen en deze gebruiken om gebruikers te sturen in hun gedrag en in hun keuzes. Gebruikers worden hiermee kwetsbaar voor winstgedreven inmenging in domeinen waarin je dat redelijkerwijs niet verwacht of waarin dat ongewenst is. Gepersonaliseerde feedback is aantrekkelijk, maar ook een heel krachtige, manipulatieve technologie.

Zoals we hebben gezien staat met de schending van privacy ook autonomie op het spel. Privacy beschermt de mogelijkheid van een autonoom leven. Hoe meer informatie we afstaan (of van ons wordt verzameld), hoe kwetsbaarder we worden voor manipulatie, sturing en uniformiteit, door overheden of bedrijven. Surveillance staat op gespannen voet met een democratie vanwege de asymmetrische machtsverhouding die surveillance impliceert en de mogelijkheid tot manipulatie van gebruikers of burgers.

We zien in de samenleving echter een trend ontstaan om steeds meer besluitvorming in allerlei sociale domeinen over te laten aan door big data gedreven algoritmes. Deze big data worden verzameld met behulp van doorlopende en intensieve surveillance. De 'algocratie' sluit dus goed aan op Zuboffs waarschuwing voor het surveillance-kapitalisme, waarin bedrijven enorm veel geld verdienen aan deze slimme algoritmes. In rap tempo infiltreert de marketinglogica van de *Frightful Five* sociale domeinen waar we niet willen dat deze marketinglogica gehanteerd wordt. Onderzoeker Evgeny Morozov waarschuwt dat een dergelijke samenleving een maatschappij is waarin de burger niet als vrij subject wordt gezien, of als iemand die zijn of haar eigen leven kan vormgeven en veranderen, maar als een categoriseerbaar, maakbaar, corrigeerbaar en voorspelbaar object.

Voor een florerende deliberatieve democratie hebben we juist burgers nodig die een min of meer autonoom leven kunnen leiden. Voor een autonoom leven is het noodzakelijk dat je tot op zekere hoogte je eigen beslissingen kunt maken en je eigen conceptie van het goede leven kunt ontwikkelen en nastreven. Privacy helpt ons daarbij. Privacy houdt in dat we redelijke verwachtingen moeten kunnen vormen over wie er zich kan bemoeien met onze informatie

'Gepersonaliseerde feedback is aantrekkelijk, maar ook een heel krachtige, manipulatieve technologie'

en beslissingen. Als dat niet lukt, voelen we ons aangetast in onze vrijheid. Bij het vormen van onze politieke keuzes willen we behandeld en gerespecteerd worden als competente beslissers. We willen niet dat dit proces gestuurd en gestructureerd wordt op basis van marketinglogica en de psychologische oorlogsvoering waar marketing gebruik van maakt.

In een interview met de Britse krant *The Observer* onthult Christopher Wylie, voormalig medewerker bij Cambridge Analytica, dat hij meewerkte aan het bouwen van psychologische profielen op basis van persoonlijke data, en vervolgens deze profielen bombardeerde met gerichte, gepersonaliseerde politieke reclames die helemaal waren afgestemd op de psychologische make-up en inspeelden op de 'innerlijke demonen' van de gebruiker (overigens wordt

deze methode om mensen van gedachten te laten veranderen of ideeën te planten ook wel bij Defensie gebruikt; het staat bekend als 'informationele dominantie'). Uit de literatuur over *persuasive technology* weten we: hoe persoonlijker de berichtgeving, hoe krachtiger en effectiever de sturing. Met behulp van een slim algoritme kon Wylie vervolgens de profilering automatiseren en miljoenen gebruikers met een muisklik bereiken. Zo was Cambridge Analytica in staat gebruikers te sturen in hun feitelijke stemgedrag.

In een democratie willen we zelf delibereren en niet gemanipuleerd worden door een machtig bedrijf of een machtige politieke actor met behulp van hypernudges. We willen met argumenten overtuigd worden door partijen waarvan we deze inmenging wensen. En we willen de mogelijkheid hebben om ons terug te trekken om te reflecteren op deze deliberatie en een eigen mening te vormen. Er geldt niet voor niets stemgeheim: privacy is belangrijk voor een deliberatieve democratie.

Het is voor een democratie belangrijk dat burgers niet behandeld worden als voorspelbare subjecten van wie het gedrag berekend en gestuurd kan worden om risico's zoveel mogelijk te reduceren. Dit sluit aan op mijn eerdere opmerking over het *chilling effect*. Voor zelfrealisatie en een dynamische identiteit is het belangrijk dat burgers vrij zijn om te experimenteren met ideeën en opties. Dat ze kunnen afwijken van de norm, de minder bewandelde paden kunnen kiezen, het recht hebben om 'ongehoorzaam' te zijn en juist te doen wat *niet* goed voor ze is. In een wereld waarin hypernudges een steeds grotere rol gaan spelen, worden de mogelijkheden voor spontaniteit en toevalligheid steeds beperkter. Een florerende democratie is gebaat bij een diversiteit aan concepties van het goede leven, zodat er idealiter altijd discussie is en niet één wereldbeeld domineert. Deze alternatieve ideeën komen alleen tot stand als je mensen vrij laat om te experimenteren.

'Het is voor een democratie belangrijk dat burgers niet behandeld worden als voorspelbare subjecten'

Verder past het bij een democratie dat we elkaar aansprakelijk kunnen houden. Technolibertariërs zoals we die veel vinden in Sillicon Valley zijn wars van overheidsinmenging. De reden is waarschijnlijk eerder pragmatisch dan ideologisch. De traagheid van de bureaucratie remt volgens technologieoptimisten de technologische innovatie — en, natuurlijk, hun inkomsten. Veel domeinen in de maatschappij zouden geoptimaliseerd kunnen worden met behulp van big data-technologieën.

Toegegeven, er valt waanzinnig veel aan te merken op de overheid; de traagheid van overheidssystemen is vaak om horendol van te worden. Maar dat komt ook omdat de overheid toestemming vraagt, zaken checkt en haar handelingswijze openbaar maakt. Veel traagheid is een gevolg van het feit dat we willen dat de overheid aansprakelijk kan worden gehouden, en dat we haar verantwoordelijk willen kunnen houden voor haar beslissingsprocedures. Monopolisten als Facebook kunnen op elk moment dat zij dat wensen hun voorwaarden en praktijken

wijzigen, al naar gelang de waarde of het belang dat ze op dat moment wensen te bevorderen. Gebruikers zitten wat dat betreft altijd in een afhankelijke positie en hebben weinig middelen om zich te verzetten of om Facebook ter verantwoording te roepen. De ironie wil dat je misschien zelfs kan beargumenteren dat de zogenaamde libertariërs gevaarlijk dichtbij de uitwassen komen van het paternalisme waar ze zich zo graag tegen af willen zetten.

Misschien dat Facebook door sommigen aanvankelijk nog kon worden gezien als een Grote Vriendelijke Reus, maar sinds de Amerikaanse verkiezingen is wel gebleken hoe precair, ongelijk en gevaarlijk deze machtsrelatie precies is. Het wordt tijd om gebruikers middelen en alternatieven aan te bieden waarmee ze zich kunnen verzetten, en om paal en perk te stellen rondom de domeinen waarvan we niet willen dat *Facebook and friends* erin rondneuzen.

© AUTEUR
MARJOLEIN LANZING

LITERATUUR

• **Allen, A.L.** (1988), *Uneasy Access: Privacy for Women in a Free Society*. Totowa: Rowman and Littlefield.
• **Brey, P.** (2006), Freedom and privacy in Ambient Intelligence. *Ethics and Information Technology* 7, 157-166.
• **Hausman, D.M. en Welch, B.** (2010). Debate: To nudge or not to nudge. *The Journal of Political Philosophy*, 18 (1), 123-136.
• **Mittelstadt, B. en Floridi, L.** (2016), The Ethics of Big Data: Current and Foreseeable Issues in Biomedical Contexts. *Science and Engineering Ethics* 22, 303—341.
• **Nissenbaum, H.** (2010), *Privacy in context: Technology, policy, and the integrity of social life.* Stanford Palo Alto: Stanford University Press.
• **Nys, T. en Engelen, B.** (2016). Judging Nudging: Answering the Manipulation Objection. *Political Studies,* 65 (1), 1-16.
• **Pasquale, F.** (2015), *The Black Box Society: The Secret Algorithms that Control Money and Information.* Cambridge, MA: Harvard University Press.
• **O'Neil, C.** (2016), *Weapons of Math Destruction*: *How Big Data Increases Inequality and Threatens Democracy.* New York: Crown Publishing Group.
• **Roessler, B.** (2005), *The Value of Privacy*. Cambridge: Polity Press.
• **Schwab, K.** (2017), Made you click: meet the AI lurking in your inbox. *FastCoDesign*. Web, 8 maart 2017.
• **Thaler, R.H en Sunstein, C.R.** (2008), *Nudge*: *Improving Decisions about Health, Wealth, and Happiness.* New Haven, Londen: Yale University Press.
• **Thaler, R.H.** (2015), The Power of Nudges, for Good and Bad. *The New York Times*. Web, 31 oktober 2015.
• **Van den Berg, B.** (2016), Coping with Information Underload. In: Hildebrandt, M. en Van den Berg, B. (red.), *Information, Freedom and Property*. New York: Routledge, 173-198.
• **Yeung, K.** (2017), 'Hypernudge': Big Data as a mode of regulation by design, *Information, Communication & Society*, 20:1, 118-136.