

DIGITALE REVOLUTIE

Een politiek antwoord op de datamacht van techreuzen
en controlestaten

Kees Verhoeven

D66

“
These are the days of miracle and wonder
This is the long distance call
The way the camera follows us in slo-mo
The way we look to us all, oh yeah
”

Boy in the bubble - Paul Simon

Auteurs:

Kees Verhoeven

Marijn van Vliet

Janne Gerritsen

Hoe de digitale droom een machtsverschuiving blijkt te zijn

De grote belofte van het internet

In 1986 had Paul Simon niet kunnen bevroeden dat we met de ontwikkeling van het internet en digitale technologieën daadwerkelijk in tijden van wonderen en verwondering zouden aanbellen. De mogelijkheden van deze technologieën zijn haast eindeloos. Het brengt vrienden en familie dichterbij, helpt bij het opsporen en genezen van ziekten als kanker of dementie en geeft iedereen toegang tot alle informatie die de mensheid ooit heeft verzameld. We hebben toegang tot een ongekende rijkdom aan muziek, film en andere kunst. We kunnen overal ter wereld de weg vinden met Google Maps, makkelijker reizen boeken met Booking.com en overal in de wereld betalen met Apple Pay. En de toekomstige technologische mogelijkheden rijken nog verder. Veel verder.

Maar digitalisering zou de samenleving ook op een andere manier fundamenteel veranderen.

In de begintijd van het internet klonk de stellige belofte dat het de wereld zou openen, de mensheid zou verbinden, welvaart beter zou verdelen, democratieën zou versterken en individuen vrijer zou maken. Mensen zouden vrij informatie kunnen delen, ideeën uitwisselen en zichzelf ontdekken. Een supersnelweg, een marktplaats van ideeën waarop iedereen gelijk zou zijn, gevrijwaard van overheidsbemoeienis en machtige tussenpersonen.

Dit wenkende perspectief, techno-optimisme of zelfs *techno-utopisme*, is al sinds de jaren 90 van de vorige eeuw het blinkende goud, het heilige geloof van Silicon Valley. Iedere ondernemer, startup en tech-gigant zou 'de wereld veranderen' met disruptieve technologieën. Waarbij men maar moest aannemen dat ze de wereld ten goede zouden veranderen; dat nieuw en modern in de praktijk ook echt beter zou zijn. De woorden van Mark Zuckerberg, CEO van Facebook, toen zijn bedrijf naar de beurs ging spraken boekdelen: *"Facebook was not originally created to be a company. It was built to accomplish a social mission – to make the world more open and connected."*¹

De datamacht van techreuzen en overheden

Als we die utopische bril afzetten en kritisch kijken naar de gevolgen van digitalisering is er veel meer aan de hand dan de zichtbare kant van blinkende gadgets, fraaie platforms en handige apps. Het verborgen karakter van het internet, de ongreepbaarheid van veel technologieën en de sluipende gestalte van digitalisering² verhullen dat (private) verdienmodellen en (publieke) controlesystemen de oorspronkelijke belofte van vrijheid hebben doorkruist. De digitale droom is niet uitgekomen. Sterker nog, de digitale droom verandert langzaam in een nachtmerrie in de vorm van een machtsverschuiving. Door de groeiende macht van techreuzen en overheden maakt het internet ons juist minder vrij. De technologie die ons dichterbij elkaar moest brengen, duwt ons verder uit elkaar. De technologie die informatie vrijuit moest verspreiden is een motor van machtsconcentratie en desinformatie geworden.

Deze maatschappelijke verandering is fundamenteel maar ook grotendeels onzichtbaar. Daarbij realiseren we ons onvoldoende hoeveel van ons leven is gedigitaliseerd. Onze dagelijkse routine wordt bepaald en in data gevat door digitale technologie. Het moment dat we wakker worden gemaakt door onze smartphone, het water dat uit de douche komt, de auto of trein die ons naar het werk brengt, het contact met vrienden en familie, het betalen van de boodschappen en de verwarming thuis; alles is verbonden via de digitale snelweg. Al deze aspecten van ons dagelijks leven worden vastgelegd en opgeslagen. Een permanent dossier waarin staat welke informatie we opzoeken, met wie we contact hebben, onze geartheid, onze politieke voorkeur, onze GPS-bepaalde locatie. Alles -van onze favoriete kattenfilmpjes tot en met de meest intieme details van ons leven- is gedigitaliseerd en opgeslagen door bedrijven en overheden.

De verzameling van al die persoonlijke data heeft geleid tot een geleidelijke, maar grote verschuiving van macht. Met mensen als verliezers en grote bedrijven en overheden als winnaars. Amerikaanse techreuzen als Facebook, Amazon, Apple, Google en hun Chinese evenknieën Tencent, Alibaba, Huawei en Baidu³ hebben een megamacht in onze samenleving. Ze weten alles over ons (*datamacht*); ze bepalen wat we zien (*mediamacht*) en ze domineren de markt (*marktmacht*). Dit vormt een maatschappelijke machtspositie die niet zelden misbruikt wordt om mensen te beïnvloeden, informatie te filteren, kleine makers te onderdrukken, personeel te verwaarlozen, concurrenten te weren en belasting te ontlopen. Bovendien worden de platforms van deze bedrijven misbruikt door derden om verkiezingen te manipuleren of om angst en twijfel te zaaien over vaccinaties of klimaatverandering. Zo is dus een macht ontstaan die gebruikt wordt tegen mens en maatschappij.

Intussen zien ook overheden de wereld door de bril van techno-utopisme. Overheden verzamelen, koppelen en analyseren steeds vaker en steeds meer data. Allerlei overheidsdatabases met daarin ID-gegevens, woongegevens en belastinggegevens worden gedigitaliseerd, gekoppeld en geanalyseerd op fraude of criminele activiteiten. Dat klinkt misschien mooi en efficiënt, maar heeft een groot effect op onze samenleving.⁴ Een van onze grondrechten is dat de overheid niets te zoeken heeft in ons privéleven, tenzij we ergens van verdacht worden. Dit grondrecht wordt met al deze data-analyses omgedraaid: we zijn bij voorbaat verdacht, tenzij de computer ons vrijspreekt. We lijken te vergeten dat dit grondrecht essentieel is voor onze vrije, democratische rechtstaat en dat het ons beschermt tegen willekeur, discriminatie en onderdrukking.

De politieke noodzaak om in te grijpen

Aanvankelijk was het idee dat de charme van het internet ook was dat de overheid er weinig over te zeggen had. Bovendien was de leidende gedachte, bij monde van Bill Clinton en Al Gore aan het begin van dit millennium, dat het reguleren van het internet ongeveer hetzelfde was als een pudding aan de muur spijkeren. Als je het al zou willen, dan zou het je niet lukken.⁵ Dat dit niet juist is, is bewezen door landen als Rusland, Turkije en China die het internetgebruik vergaand reguleren en controleren.

Later mengde de politiek, ook in liberale democratieën, zich wel in het internetdebat, al verliep dat stroef. Een gebrek aan prioriteit, een digitale kennisachterstand, een beperkte zeggenschap over de vaak private infrastructuur van kabels, servers en routers en versnippering over verschillende ministeries en bestuurslagen, vormden vaak belemmeringen voor een actieve rol van politici.

Anders dan tien jaar geleden staan tegenwoordig tal van digitale issues op de politieke agenda. De digitalisering van de overheid roept vragen op over de toegankelijkheid van de dienstverlening en de kosten van ICT-projecten. De aanleg van de vijfde generatie nieuw internet (5G), de snelle groei van apparaten met een internetaansluiting (IoT) en het hacken door de overheid via onbekende softwarekwetsbaarheden (*Odays*) hebben gevolgen voor de veiligheid van onze vitale infrastructuur en dus de stabiliteit van onze samenleving. Opkomende technologieën bieden grote kansen voor het verbeteren van de zorg, het onderwijs, de industrie en de landbouw. Toch zorgt de achterblijvende innovatiekracht van Nederland en de Europese Unie voor een groot risico in onze economische en geopolitieke positie ten opzichte van China en de Verenigde Staten.

Stuk voor stuk belangrijke thema's die mens en maatschappij raken. Maar het hoofdthema van nu, de groeiende macht van techreuzen en overheden ten opzichte van mensen, is te lang onderbelicht gebleven. De afgelopen jaren ging het politieke debat vooral over het achterhaalde auteursrecht, uit de hand lopende IT-projecten, privacy-schendingen, datalekken, veiligheidsrisico's, online fraude en de druk op onze mondiale concurrentiepositie. Maar het moet ook gaan over het bewaken van onze vrijheid, onze democratie en onze rechtstaat in het digitale tijdperk, het beschermen van menselijke waarden tegen de macht van techreuzen en controlestaten. Technologie wordt vaak beschreven als machtsfactor in *geopolitieke termen* van veranderende machtsverhoudingen tussen China, de VS en Europa. Dat is terecht maar we zien data en digitale technologie onvoldoende in *politieke termen* van veranderende machtsverhoudingen in onze samenleving; tussen mensen, overheden en bedrijven. Dat moet veranderen. Voordat het te laat is.

Het is nu of nooit

Wie terugblijkt op de afgelopen tien jaar ziet de immense veranderingen die in minder dan een decennium hebben plaatsgevonden. In 2011 was Hyves nog groter dan Facebook. Veiligheidsdiensten werden bekritiseerd over te veel telefoontaps. En de Tweede Kamer debatteerde over een downloadverbod. We staan nu aan de vooravond van een nieuwe technologische revolutie. Systemen worden steeds slimmer, technologieën vormen steeds meer een samenhangend geheel en de samenleving wordt steeds verder gedataficeerd.⁶ Er is vergaande vooruitgang op het gebied van *quantumcomputing*, nanotechnologie, robotica en sensortechnologie. Maar vooral kunstmatige intelligentie (*machine learning*, *deep learning*) zal een enorme vlucht nemen. Waar de toepassingen nu nog relatief smal (specifiek) zijn, zullen ze snel meer omvattend (generiek) worden en is de stap naar algemene kunstmatige intelligentie (bovenmenselijk) op de langere termijn niet uit te sluiten.

Vandaag de dag zorgt het samenspel van het exponentieel groeiende internet der dingen (*wareables*, *health-apps*) en enorme opslagcapaciteit (cloudtechnologie) voor *big data* die met enorme computerkracht en zelflerende machines bewerkt worden. Dit klinkt technisch en abstract maar het is in feite heel simpel en concreet. In de toekomst wordt het nog makkelijker om nog meer data te verzamelen, te koppelen en te analyseren. Bijvoorbeeld door het toepassen van gezichtsherkenning op camerabeelden. Er zullen steeds meer verdergaande toepassingen zijn, zoals *deepfake*⁷ technologie waardoor feit en fictie minder goed van elkaar te onderscheiden zijn. Techreuzen en overheden zullen steeds dieper in onze levens kunnen treden. Als we niet oppassen, gebeurt dat zonder dat we daar grip op hebben.

Zonder dat we een vrije keuze of inspraak hebben. Zonder dat we ons recht kunnen halen. Daarom moeten we nu ingrijpen; we kunnen niet wachten.

Dit pamflet is geschreven om de sluier van techno-utopisme af te trekken. De digitale sluipmoordenaar moet ontmaskerd worden; om mensen te waarschuwen voor de geleidelijke en haast onzichtbare, maar fundamentele verandering van onze samenleving als gevolg van digitalisering. De invloed van digitalisering op onze samenleving is vooralsnog positief onder de streep. Maar als we haar niet voldoende afremmen, bijsturen en begrenzen slaat die balans de verkeerde kant op.

Niets minder dan onze vrije, democratische rechtstaat staat op het spel. Het is tijd voor een digitale revolutie. We moeten voorkomen dat tijden van wonderen en verbazing omslaan in tijden van catastrofes en vervreemding.

Hoe onbegrensde mogelijkheden het internet tot grote belofte maakten

“

**These are the days of miracle and wonder,
This is the long distance call.**

Boy in the bubble - Paul Simon

”

Techno-utopisme

In 1993 maakte de wereld kennis met de eerste webbrowser, Mosaic. Het portaal naar het internet. Een nieuwe virtuele wereld ging open: de online wereld. Het stelde mensen in staat om via de computer contact te maken met mensen over de hele wereld. Hiervoor werd die grote kast in de hoek van de kamer vooral gebruikt voor het typen van teksten, het vullen van spreadsheets of het spelen van spelletjes. Ondernemers, bedrijven en investeerders sprongen erop. Google, MSN, EBay en Yahoo stammen allemaal uit die tijd. Een ongekend hoogtepunt dat eindigde in de 'dotcomcrisis' van 2000, maar die de vooruitgang in digitale technologieën en het internet niet stopte, hooguit onderbrak en even afremde.

Digitalisering heeft ons immers veel vooruitgang gebracht. Het gemak waarmee we contact hebben met vrienden en familie over de hele wereld. De toegang tot ongekeende hoeveelheden informatie via Google, muziek op Spotify en films en series op Netflix. Niet meer eindeloos lang in de rij hoeven te staan bij de bank en veiliger geldtransport dankzij internetbankieren. De zelfrijdende auto's, *drones* en satellieten. GPS, of het Europese Galileo, dat we dagelijks gebruiken om van A naar B te komen. Digitalisering is compleet verweven met ons dagelijks leven. Van een scheiding tussen *cyberspace* en onze fysieke leefwereld, die sommigen suggereren, is dan ook geen sprake.

Digitalisering heeft ook veel betekend voor wetenschappelijk onderzoek. Ongekeende hoeveelheden data kunnen worden geanalyseerd door supercomputers om antwoorden te vinden op vragen over het ontstaan van ons universum of om geneesmiddelen voor kanker te ontdekken. Om nog maar te zwijgen over de enorme economische kansen voor Nederland; het digitale knooppunt AMS-IX, automatisering in de haven van Rotterdam, het succes van ASML, jonge bedrijven als Adyen, Elastic, Hackerone, The Next Web en Booking.com.

Maar het optimisme in de begintijd van het internet was niet alleen gericht op het verdienen van geld of het verbeteren van ons fysieke welzijn. 'Don't be evil' was lang het motto van Google. Internetondernemers geloofden heilig in de waarde van het verbinden van de wereld. Het internet als vrijplaats voor ideeën, los van overheidsbemoeienis of controle. De gedachte is misschien nog het beste omschreven door Mark Zuckerberg toen Facebook naar de beurs ging:

"Facebook was not originally created to be a company. It was built to accomplish a social mission – to make the world more open and connected. At Facebook [...] we often talk about inventions like the printing press and the television – by simply making communication more efficient, they led to a complete transformation of many important parts of society. They gave more people a voice. They encouraged progress. They changed the way society was organized. They brought us closer together."⁸

Simpelweg het verbinden van mensen zou genoeg moeten zijn om vooruitgang te stimuleren; om samenlevingen te transformeren. Het zou mensen een stem geven, een manier om buiten de 'gatekeepers' van informatie hun mening te uiten. Zo zouden deze techno-utopisten de wereld verbeteren door mensen dichterbij elkaar te brengen. De wereld zou verbonden en gelijk zijn. De economie zou eeuwig groeien. De hemel zou op aarde zijn.

Hoe de keerzijde van de digitale medaille langzaam zichtbaar werd

“

The way we look to a distant constellation
That's dying in a corner of the sky.

Boy in the bubble - Paul Simon

”

Privacyproblemen, economische dilemma's en veiligheidsrisico's

Zoals altijd bracht het heilige geloof niet de voorspelde verlichting. Zoals zo vaak met grote beloftes liep het in werkelijkheid anders. Het gedroomde scenario van vrijheid en verbinding bleek een weerbarstige praktijk te kennen. Langzaam maar zeker ontstonden er scheurtjes in het gepolijste imago van het internet. Silicon Valley bleek vooral oplossingen te bieden voor niet-bestaande problemen om hier zelf het meest van te profiteren.

Een jaar na de introductie van de eerste webbrowser werd de cookie uitgevonden en - onzichtbaar voor het grote publiek - geïntroduceerd via de Netscape (1994) en Internet Explorer (1995) browsers. In eerste instantie was dit vooral een oplossing om het makkelijker te maken om online te winkelen; producten stonden ook de volgende dag nog in je online winkelmandje. Maar het was vooral de eerste stap naar het volgen van internetgedrag van mensen, het huidige verdienmodel van Google en Facebook. Pas twee jaar na de introductie van de cookie werd het gebruik ervan bekend, wat leidde tot veel ophef over de gevolgen op de privacy van mensen.

De uitvinding van de cookie markeert ook het begin van een tijdperk vol grote privacy-schandalen. Van het Financial Times-artikel uit 1996 dat het bestaan van cookie bekend maakte bij het grote publiek tot de vele Facebook-schandalen van de afgelopen jaren (met als hoogtepunt de manipulatie van gegevens van honderdduizenden Facebook-gebruikers door het Brits-Amerikaanse bedrijf Cambridge Analytica) en van de Snowden onthullingen tot het Yahoo-datalek van 3 miljard accounts.⁹

Met de opkomst van het internet kwamen ook economische dilemma's naar boven. In 1999 zag het beroemde Napster het licht. Hiermee konden mensen onderling bestanden uitwisselen, zoals muziek en films. Dit was het begin van jarenlange discussies over illegaal downloaden en piraterij, DNS-blokkades van Pirate Bay, de opkomst van Digital Rights Management en Bittorrent. Zo zijn er de afgelopen jaren nog tal van debatten geweest over de economische gevolgen van digitalisering. Het debat over netneutraliteit spitste zich toe op de gevolgen van gratis chatverkeer voor de Telecombedrijven die hun geld verdienen met sms'jes. Ook de ruimtelijke en sociale gevolgen van de digitale economie vroegen om aandacht.

Leegstand als gevolg van online shoppen en thuiswerken. Maar ook veranderende werkgelegenheid doordat briefpost en fototoestellen werden vervangen door e-mail en smartphones.

Naast privacyproblemen en economische dilemma's zien we de laatste jaren ook de keerzijde van digitalisering op het vlak van veiligheid. Op 10 oktober 2012 maakte de Canadese tiener Amanda Todd een einde aan haar leven. Ze werd digitaal gechanteerd met naaktfoto's die door de Nederlandse Aydin C waren buitgemaakt door zich voor te doen als tiener.¹⁰ In 2008 werd een 22-jarige man uit Culemborg veroordeeld omdat hij jarenlang webcams van jonge meisjes had gehackt en ze met de naaktbeelden had gechanteerd¹¹. Dit zijn zeer pijnlijke voorbeelden van de keerzijdes van alom aanwezige digitale apparaten als webcams en de inherente onveiligheid daarvan.

In juni 2016 stonden ineens de kranen van APM Terminals in de Rotterdamse haven stil. Een *ransomware* aanval genaamd Notpetya had de digitale systemen van het bedrijf platgelegd waardoor vrachtwagens en schepen dagenlang hun lading niet kwijt konden met miljoenen euro's aan schade tot gevolg. In totaal kost cybercriminaliteit Nederland ongeveer 10 miljard per jaar.¹² Maar volgens onderzoeken van de Rekenkamer, instituten als de Wetenschappelijke Raad voor het Regeringsbeleid (WRR) en het Rathenau Instituut, het Cybersecuritybeeld en de jaarverslagen van inlichtingendienst AIVD kan de gebrekkige digitale veiligheid van Nederland leiden tot maatschappelijke ontwrichting.

Een machtsverschuiving weg van mensen

Geen van de internet-ondernemers uit Silicon Valley had een idee van de enorme invloed en negatieve gevolgen van hun uitvindingen op onze samenleving. De effecten op het gebied van privacy, economie en veiligheid werden niet gezien, ondanks vergelijkbare industriële revoluties en technologische ontwikkelingen (stoommachines, elektriciteit) die leidden tot grote maatschappelijke vraagstukken. De decentrale opzet, de relatieve onzichtbaarheid en de complexe structuur van het internet speelden hierin een belangrijke rol.

Jazeker, het is het internet inderdaad gelukt om mensen toegang te geven tot vrijwel alle kennis die ooit door de mensheid is vergaard. En dat is een gigantische prestatie. Tegelijkertijd is de belofte van het vergroten van vrijheid gebroken door een parallelle ontwikkeling die over het hoofd werd gezien en die niet te voorspellen was. Namelijk de geleidelijke verschuiving van macht als gevolg van data en technologieën die steeds indringender, intiemer en intimiderend worden; een machtsverschuiving weg van mensen, naar overheden en bedrijven. Met gevolgen voor onze vrijheid, onze democratie en onze rechtstaat. Ofwel: de fundamenten van onze maatschappij. De genoemde schaduwkanten van digitalisering op het gebied van privacy, economie en veiligheid zijn ernstig genoeg en alle reden voor politiek debat. Maar het gaat hier om de fundamentele keerzijde van digitalisering. Een ontwikkeling die raakt aan politieke kernzaken als machtsbalans, vrijheid, democratie en rechtvaardigheid.

Om die ontwikkeling goed te kunnen bevatten is het essentieel om eerst terug te gaan naar de basale principes die aan de basis van onze maatschappij staan.

Waarom digitalisering een prangend politiek thema is

“

It's a turn-around jump shot
It's everybody jump start
It's every generation throws a hero
up the pop charts.

Boy in the bubble - Paul Simon

”

Macht, tegenmacht en de scheiding der machten

De scheiding der machten, ofwel de *trias politica*, is een van de basisprincipes van onze rechtstaat. De Franse filosoof Charles baron de Montesquieu zag dat personen of organisaties met veel macht vaak misbruik maken van die macht en de vrijheid van anderen schenden. Montesquieu zei hierover:

“If the legislative and executive authorities are one institution, there will be no freedom. There won't be freedom anyway if the judiciary body is not separated from the legislative and executive authorities.”

Zonder scheiding der machten, geen vrijheid. Zonder controle op macht geen vrijheid. Zonder tegenmacht geen vrijheid.

Door de jaren heen zijn er meer machten toegevoegd aan de drie machten (wetgevende, uitvoerende en rechterlijke) van Montesquieu. Deze additionele machten worden ook wel aangeduid met de term 'vierde macht'. Beroemd politiek theoreticus Max Weber heeft uitgebreid geschreven over de ambtenarij als bron van macht. Anderen hebben de macht van lobbyisten en adviesbureaus aangedragen. Maar er wordt internationaal vooral veel geschreven over de media als vierde macht.

De term is toegeschreven aan Edmund Burke die het gebruikte tijdens een parlementair debat: *“There were Three Estates in Parliament; but, in the Reporters' Gallery yonder, there sat a Fourth Estate more important far than they all.”* Media geven immers voor een belangrijk deel de communicatie tussen politiek en mensen vorm. De traditionele drie machten hebben directe macht. In het geval van media gaat het vooral om indirecte macht en de invloed op de overtuigingen van mensen. Voorheen waren het de grote mediabedrijven die deze rol innamen. Tegenwoordig spelen technologische bedrijven als Google, Twitter en Facebook (met hun nieuwsplatforms, zoekmachines en chatdiensten) een soortgelijke rol in de verspreiding van informatie. Zij hebben de mediamacht steeds verder overgenomen.

De macht verschuift geleidelijk en onzichtbaar

Macht is een thema dat cruciaal is voor vrijheid, democratie en recht. Verschuivende mediamacht en marktmacht en dus veranderende maatschappelijke macht als gevolg van digitalisering vormt daarom een veel serieuzer risico dan de incidenten die we tot nu toe hebben gezien op het gebied van economie, privacy en veiligheid. Verschuiving van macht kan een fundamentele bedreiging betekenen voor onze vrijheid, onze rechtstaat en onze democratie. Maar wat is macht? Wat maakt een persoon of entiteit machtig? Hoe wordt macht uitgeoefend? En welke rol spelen digitale technologieën daarin?

In zijn doorwrochte boek 'Future Politics' (2018) gaat Jamie Susskind in op de relatie tussen technologie en macht. Kortweg beschrijft hij hoe digitale technologie ingrijpt op informatie en communicatie en daarmee op systemen van samenwerking, coördinatie en controle. Dit heeft gevolgen voor het kunnen uitoefenen van macht door zowel techbedrijven als overheden. Want data, software en algoritmes maken het mogelijk om mensen te dwingen, te onderzoeken en te sturen. Deze machtsverschuiving maakt dat technologie dus de vrijheid, democratie en sociale rechtvaardigheid in onze samenleving raakt en daarmee een belangrijk politiek thema is.¹³ Susskind hanteert de volgende definitie van macht:

"A person or entity is powerful to the extent that it has a stable and wide-ranging capacity to get others to do things of significance that they would not otherwise do, or not to do things they might otherwise have done."

Macht is dus het vermogen hebben om anderen dingen te laten doen die ze anders niet zouden doen, of om anderen dingen niet te laten doen die ze anders misschien wel hadden gedaan. Maar hoe dan?

"Kennis is macht." - Francis Bacon

Al honderden jaren wordt geschreven over de relatie tussen kennis en macht; van Francis Bacon tot Michel Foucault. Foucault concludeerde dat macht gebaseerd is op kennis en gebruikmaakt van kennis. Maar ook dat macht kennis kan vormgeven. In de digitale wereld is data macht. Die data is veelal kennis over mensen: wie we zijn, wat we doen en waar we zijn. Data is een vorm van macht die gebruikt wordt om kennis van mensen te beïnvloeden. Denk aan de algoritmes van Google die bepalen wat voor informatie we zien.

De belofte van digitale technologie was dat het de vrijheid van mensen zou vergroten door de toegang tot informatie makkelijker te maken voor iedereen. Dat het de kennis van mensen en daarmee hun macht zou vergroten. Maar wat digitalisering vooral heeft bereikt is het vergroten van de kennis van bedrijven en overheden over mensen.

Kortom, macht is een belangrijk onderwerp in een samenleving. Zeker in een vrije, democratische rechtstaat die afhankelijk is van de scheiding der machten, van machtsbalans en van tegenmacht. Ongecontroleerde macht leidt immers tot onvrijheid en onrechtvaardigheid. Daarnaast is het belangrijk om te kijken naar bronnen van macht. In het digitale domein geldt misschien wel meer dan ooit dat kennis macht is en dat die kennis is gevat in data.

Hoe vergroten bedrijven en overheden hun kennis over mensen? Hoe vergroot dit hun macht en hoe gebruiken ze die macht?

Hoe techbedrijven met hun commerciële belangen steeds machtiger worden

“

**Staccato signals of constant information
A loose affiliation of millionaires
And billionaires and baby**

Boy in the bubble - Paul Simon

”

Datamacht

De hoeveelheid data die bedrijven als Facebook, Amazon en Google¹⁴ over mensen hebben is ongekend. Nog nooit zijn zoveel aspecten van de levens van zoveel mensen vastgelegd als nu. Via zoekopdrachten op Google, likes op Facebook en tweets op Twitter. Maar ook via de koppeling van allerlei databestanden verzamelen bedrijven een ware schat aan kennis. Over wat we denken en leuk vinden, over angsten en wensen. Met wie we contact hebben. Geaardheid, politieke voorkeuren en afkomst. Huisadres, naam en woonplaats. Onze hartslag, locatie en medische gegevens. We geven het allemaal weg aan bedrijven. En we geven ze zo kennis over de meest intieme onderdelen van onze levens.

Al die gegevens creëren een zeer gedetailleerd beeld van ons. Hierdoor kennen deze bedrijven ons feitelijk beter dan onze vrienden en familie. Volgens onderzoek van Cambridge en Stanford kent Facebook ons na 10 likes al beter dan collega's, na 70 likes beter dan onze vrienden en na 150 likes beter dan onze familie.

Alleen al het hebben en verzamelen van deze data zelf is een vorm van macht (we noemen het hier datamacht¹⁵) die mensen minder vrij maakt. Michel Foucault schreef veel over de relatie tussen kennis en macht en vooral over 'disciplinaire macht'¹⁶, die niet wordt uitgeoefend door dwang of dreiging, maar door middel van disciplinaire 'apparaten'. Hij concludeerde het volgende over dit type macht: “[it] reaches into the very grain of individuals, touches their bodies and inserts itself into their actions and attitudes, their discourses, learning processes and everyday lives”. Waar Foucault het in deze context vooral had over scholen, gevangenissen en klinieken, zou je kunnen zeggen dat techreuzen ook een dergelijke rol hebben.

Het feit dat we weten dat we 'gevolgd' worden, of dat anderen veel over ons weten, maakt dat we ons anders gedragen. Het zorgt ervoor dat we minder snel dingen doen die door de maatschappij worden gezien als 'slecht' of schandelijk. Zo zorgt dit soort datamacht ervoor dat mensen zichzelf censureren en daarmee minder vrij zijn om zichzelf te zijn. Kun je je nog vrij ontwikkelen als een -overigens zelf onzichtbare- macht continu over je schouder meekijkt?

Waarom verzamelen bedrijven eigenlijk zoveel informatie over ons? Het verdienmodel van deze bedrijven is de grootste boosdoener (maar niet de enige factor). Google verdient 85% van zijn omzet uit advertenties, Facebook zelfs 99%. Dat werkt als volgt: data helpt om meer clicks op advertenties te krijgen. Want naarmate je meer over iemand weet, groeit de kans dat de gekozen advertentie aansluit op zijn of haar interesses en daarmee de kans dat iemand op deze advertentie klikt¹⁷. En meer data helpt om ervoor te zorgen dat mensen zoveel mogelijk tijd doorbrengen op je website of app. Mensen zien namelijk content die ze willen zien. Berichten die het verleidelijk maken om meer tijd door te brengen op de website of app. Want hoe langer mensen op Facebook zitten, hoe meer advertenties getoond kunnen worden en hoe meer geld Zuckerberg kan verdienen.

Het terugpakken van de macht en dus de vrijheid van het individu zal sterk afhangen van de aanpak van dit verdienmodel.

De publiek-private verhoudingen in de Verenigde Staten, China en de Europese Unie

Naast de bewuste commerciële belangen van de techbedrijven spelen er nog twee andere mechanismen waar Amy Webb in haar boek "The Big Nine" indringend op wijst. Allereerst is dat het gegeven dat techbedrijven in de Verenigde Staten vaak kleine, homogene groepen mensen (*'tribes'*) zijn die ontstaan in universiteitsgebouwen en op bedrijfscampussen. Dit zijn vaak weinig diverse groepen *engineers* met een hoog gehalte aan zogenaamde *hardskills* (informatica, programmeren). Zij geven met hun software en technische vondsten richting aan de toekomst, vaak met goede intenties maar grotendeels geïsoleerd en ongecontroleerd en op grote afstand van gewone mensen¹⁸. Vanwege hun eensoortigheid zijn ze gevoelig voor vooringenomenheid, eenkennigheid en geslotenheid. Zo krijgt het ontstaan van *biases*, *bubbles* en *black boxes* dus ruim baan met nadelige gevolgen voor iedereen.

Ten tweede bevindt Silicon Valley zich in een spagaatpositie tussen Wall Street en Capitol Hill, oftewel de aandelenbeurs en de Amerikaanse politiek. Dit leidt tot grote druk op snelle en tastbare resultaten met als gevolg grove inschattingfouten en schandalen zoals Microsofts mislukte chatbot Tay op Twitter¹⁹ of het Maven-project waarbij Google nauw samenwerkt met het Pentagon tegen de zin van veel medewerkers²⁰. De druk om politici en aandeelhouders tevreden te stellen versterkt de toch al aanwezige tech-cultuur van "*Built first, apologize later*" met fouten en schade als resultaat. Webb benadrukt daarom dat het internet en kunstmatige intelligentie veel meer als een publiek goed behandeld zouden moeten worden.

In China is dat wel het geval maar zeker niet met gunstigere gevolgen voor de vrijheid van mensen. Daar zit de Chinese Volkspartij onder leiding van president van de Volksrepubliek Xi Jinping namelijk bovenop techbedrijven als Baidu, Alibaba en Tencent. Deze vormen een integraal onderdeel van de Chinese lange termijnstrategie om via technologie wereldmacht nummer 1 te worden²¹. De vergaande controle

en surveillance waarmee dit gepaard gaat, zoals het sociaal kredietsysteem²², onderdrukt miljoenen Chinezen. Maar als de voorziene technologische dominantie van China werkelijkheid wordt zal dit ook de westerse wereld steeds meer gaan raken.

Terwijl de overheid in de VS techbedrijven veel ruimte geeft en de Chinese overheid juist een stevige vinger in de pap heeft, is de Europese Unie meer gericht op de burger, hetgeen je terugziet in regelgeving zoals de Europese privacywet AVG. Deels is dit historisch en cultureel bepaald, deels is dit pragmatisme omdat Europa geen techreuzen kent en slechts enkele relevante platforms (Booking.com, Spotify, Zalando) binnen haar grenzen heeft²³. Er zijn mensen die stellen dat Europa leidend kan zijn in het bewaken van waarden en het stellen van regels. Maar onze marginale rol in de platformeconomie en onze achterstand in de technologie-wedloop staat dit in de weg. Daarom is het nodig dat Europa de komende jaren investeert in de ontwikkeling van een Europese techindustrie.²⁴

Mediamacht

Niet alleen het bezit van al die kennis over mensen is een vorm van macht, ook de manier waarop het wordt gebruikt is een vorm van macht. De persoonlijke data van mensen die deze bedrijven bezitten wordt namelijk gebruikt om te bepalen wat voor content zij zien. Slimme algoritmes analyseren de data om te bepalen wat voor informatie of nieuws iemand op welk moment zou willen zien. Hoewel 'willen' hier niet helemaal het goede woord is. Bedrijven weten zoveel over mensen, dat ze weten voor welke soort informatie mensen het meest gevoelig zijn.²⁵ Controle over wat mensen zien, wat voor informatie ze voorgeschoteld krijgen en wat voor nieuws ze lezen is een enorme bron van macht. Het stuurt namelijk de kennis en het beeld dat mensen van de wereld krijgen. En het beperkt mensen in hun handelen omdat ze niet weten wat ze niet weten.

Tegelijkertijd proberen grote techreuzen deze macht te ontkennen. Hand in hand met het technoutopisme dat we in hoofdstuk 1 bespraken ging een bedrieglijk soort neutraliteitsdenken. Bedrijven als Facebook of Google, maar ook minder bekende platforms als Reddit, 4chan en 8chan, zouden slechts mensen de mogelijkheden geven zich te uiten. Ze zouden zich niet bemoeien met de inhoud. Deze bedrijven zijn slechts een neutraal platform waarop mensen zich kunnen uiten zonder verantwoordelijkheid voor de gevolgen.²⁶

"People having the power to express themselves at scale is a new kind of force in the world – a Fifth Estate alongside the other power structures of society. People no longer have to rely on traditional gatekeepers in politics or media to make their voices heard, and that has important consequences." Sociale media zijn een 'vijfde macht' volgens Facebook CEO Mark Zuckerberg. Daarmee refereert hij aan een term uit de jaren 60 waarmee alternatieve media bedoeld worden en waarmee Facebook elke vorm van verantwoordelijkheid probeert te ontlopen.²⁷

Ondanks het feit dat techreuzen hun macht ontkennen en zich wentelen in een mantel van neutraliteit en ontkenning van verantwoordelijkheid, oefenen deze bedrijven wel degelijk macht uit. Facebook's algoritmes die bepalen wat mensen zien, zitten vol met bewuste en onbewuste keuzes van bedrijven die van grote invloed zijn op onze maatschappij. Het is een keuze van Google om te bepalen welke filmpjes mensen aangeraden krijgen over het ontkennen van klimaatverandering. Het is een keuze van Facebook

om politici nepnieuws te laten verspreiden via advertenties en om grote hoeveelheden nepnieuws over vaccinaties te laten circuleren. Het is een keuze van 8chan om ruimte te bieden aan rechtsextremistische geweldsverheerlijking.

Natuurlijk zijn dit moeilijke en complexe keuzes die raken aan de vrijheid van meningsuiting. Maar het zijn geen nieuwe vragen. De uitvinders van de drukpers hadden soortgelijke denkbeelden over hun rol in de samenleving. Ook zij zagen zichzelf als een neutraal platform dat niet verantwoordelijk was voor wat schrijvers opschreven. Ook al hadden ze hun bedenkingen bij sommige teksten in de boeken die ze drukten. Zonder de drukpers had Maarten Luther nooit zoveel mensen kunnen bereiken en een revolutie kunnen ontketenen. Maar diezelfde drukpers stelde diezelfde Luther in staat om boeken te verspreiden met titels als 'Over de Joden en hun leugens' en 'een waarschuwing tegen de joden'.

Door de jaren heen is de rol van uitgeverijen, kranten en radio en televisiemedia in de samenleving veranderd en wordt die sector ook gedefinieerd door wat het niet en wel wil uitgeven. Onafhankelijke redacties en statuten zorgen voor transparantie en verantwoordelijkheid.

Deze verantwoordelijkheid en transparantie ontbreken nu bij grote spelers in de digitale wereld. Met als gevolg dat de Wereldgezondheidsorganisatie waarschuwt dat vaccinatiegraden in Europa achteruit gaan en ernstige kinderziekten als de mazelen weer terug zijn, dat buitenlandse actoren met nepnieuws en trollen democratische processen beïnvloeden. We leven nu in een "post truth" wereld waarin leugens niet meer te onderscheiden zijn van de waarheid en waarin de journalistiek moet vechten om te overleven.

Journalistiek is onmisbaar in een democratie. Vrijheid kan niet zonder vrije pers. Toch wordt de vrije pers steeds verder aangetast door teruglopende inkomsten. Dat komt deels door de veranderende manier waarop mensen nieuws tot zich nemen, maar ook door de keuzes die Facebook en Google maken in hun algoritmes. Een kleine aanpassing in het algoritme van Facebook leidde tot het ontslag van 1000 journalisten bij BuzzFeed en HuffPost. Dit betekent ook dat 1000x minder menselijke afwegingen worden meegewogen.

Facebook ontloopt verantwoordelijkheid voor al het misbruik door zich uit te roepen tot vijfde macht en sloopt vervolgens de vierde macht (media) die juist essentieel is om weerstand te bieden tegen desinformatie en manipulatie.

Maar dit is niet de enige manier waarop de macht van techreuzen in de democratie voelbaar is. In 2013 publiceerden twee onderzoekers van de Universiteit van Cambridge een studie waarin ze zeiden dat ze de persoonlijkheden van mensen konden voorspellen op basis van likes op Facebook. De gevolgen waren groot. Aleksander Kogan bouwde een app waarmee hij, zonder toestemming, persoonlijke gegevens van miljoenen Amerikanen verzamelde. Diezelfde data werd later door Cambridge Analytica gebruikt om stemmers tijdens de presidentsverkiezingen van 2016 met gepersonaliseerde advertenties te overtuigen op Donald Trump te stemmen en om andere stemmers – vaak minderheden – te overtuigen niet te gaan stemmen. Een 'psychological warfare tool' noemde klokkenluider Christopher Wylie het.

De enorme hoeveelheden data die Facebook over ons bezit werden misbruikt om mensen op oneigenlijke manier te beïnvloeden op een politiek kandidaat te stemmen. Een grotere invloed op de democratie en een duidelijker voorbeeld van de enorme maatschappelijke macht van techreuzen is bijna niet denkbaar.

Marktmacht

Maar focussen we niet teveel op een paar bedrijven? Er is toch concurrentie? Voor Facebook was er Myspace en straks komt er een opvolger van Facebook. De concurrentie is groot, zeggen deze techreuzen en hun voorvechters, lobbyisten en advocaten. Dit zou mooi zijn, want dat zou betekenen dat de verschuiving van macht van mensen naar techbedrijven slechts een tijdelijke fase is. Helaas zien we steeds duidelijker dat dit een nieuwe illusie is. Daarbij heeft het verleden uitgewezen dat het doorbreken of gedeeltelijk afbreken van een industriële of technologische macht (zoals Standard Oil en Microsoft) altijd overheidsingrijpen vereist. Achterover leunen is dus geen optie.

Elke macht heeft tegenmacht nodig en elke markt heeft een strenge marktmeester nodig. Een marktmeester die het economisch spel van de markt grondig begrijpt. Een marktmeester die de spelregels handhaaft om te voorkomen dat het recht van de sterkste domineert. Die marktmeester is er in de digitale economie nauwelijks. Met als gevolg dat de grote techreuzen vrij spel hebben.

De bedrijfsmodellen waarmee grote techreuzen winst maken zijn fundamenteel anders dan voorheen. In de analoge economie betalen bedrijven en consumenten met geld. Een koffietentje koopt bonen in, neemt een barista aan en verkoopt je tegen een paar euro een verse kop koffie. Om meer winst te maken moet de eigenaar de prijs van de koffie verhogen of meer producten verkopen. Gratis koffie bestaat niet, tenzij je er op een andere manier voor betaalt.

In de digitale economie lijkt gratis koffie te bestaan. Google vraagt geen geld voor het gebruik van de zoekmachine, G-mail, Maps, Android, Chrome en Drive. Terwijl ze daar wel kosten voor maken. Ze vragen je alleen om je data bij te mogen houden. Waarop je zoekt, op welk moment van de dag je dat doet, vanaf welke locatie en meer. Ze gebruiken de data om advertenties te tonen. De gratis koffie legt Google geen windeieren. 85% van alle inkomsten van het moederbedrijf van Google kwam uit advertenties: 95,4 miljard dollar.

De digitale economie werkt op een aantal punten geheel anders dan de traditionele economie. De datamacht van de techreuzen zet ze op een gigantische voorsprong. Elke byte aan informatie maakt het algoritme steeds slimmer. Daarom blijf je eindeloos rondhangen op Facebook en weten Spotify en Netflix precies wat je wilt horen en zien. Uitdaggers, startups en kleine concurrenten die niet genoeg data hebben kunnen nooit zulke effectieve algoritmes maken. Zo sluit datamacht tegenmacht door uitdagers uit.

In 2011 was Hyves nog populairder dan Facebook in Nederland. Enkele jaren later ging het ten onder. Dat is een voorbeeld van een ander verschil: het *netwerk-effect*.²⁸ Hoe meer gebruikers er op een platform zijn, des te meer data er wordt achtergelaten, des te waardevoller het platform is. Niemand zit nog te wachten op een tweede Facebook, tweede Twitter of tweede LinkedIn app. Door het netwerkeffect dat zorgt voor optimalisatie op basis van datamacht worden de techreuzen niet meer uitgedaagd.

Het is eten of gegeten worden in de digitale economie. Om de macht te behouden en te vergroten, strijden de bedrijven niet alleen op markten maar ook om markten. Meer diensten aanbieden betekent meer data en minder concurrentie. De economische spelregels, zoals het kartelverbod of het verbod op misbruik van economisch dominante posities, horen tegenwicht te bieden. De regelgeving is alleen nog niet up-to-date voor de huidige digitale economie.²⁹

Dat het recht van de sterkste techreuzen zegeviert, komt in alle uitwassen duidelijk naar voren. Medewerkers en kleine makers worden uitgebuit en belastingplicht wordt ontlopen. De gretigheid naar advertentie-inkomsten is zo hoog, dat er liever aan desinformatie wordt verdiend dan op fatsoenlijke bedrijfsvoering wordt toegezien.

Zo zijn de techreuzen Google, Amazon, Facebook en Apple door datamacht de grote industrialisten van onze tijd geworden. En op afzonderlijke meer specifieke deelmarkten kunnen specifieke platforms zoals Netflix, Spotify, Uber en Airbnb zeer machtig zijn. Veel van deze bedrijven misbruiken hun marktmacht om hun dominante positie te behouden. Innovatieve startups worden opgekocht en onschadelijk gemaakt. Als er al een serieuze uitdager komt, dan wordt die vaak overgenomen zoals Google het platform YouTube inlijfde en Facebook diensten zoals WhatsApp en Instagram overnam. En als een uitdager de dans weet te ontsnappen, dan wordt hij gekopieerd zoals Facebook/Instagram de app Snapchat kopieerde. Op deze manier overleeft de monopolist. Dit is slecht voor innovatie, slecht voor de concurrentie en dus slecht voor ons allemaal.

De kern van de verschuiving van macht van mensen naar bedrijven ligt bij data en de steeds verdergaande verwerking ervan. Het verdienmodel van de techreuzen draait om het verzamelen van zoveel mogelijk data. Meer data betekent meer persoonlijke advertenties. Meer data betekent mensen langer kunnen vasthouden op de website of app en dus meer advertenties. Meer advertenties en persoonlijker advertenties betekenen meer geld. Meer data betekent dus gratis diensten voor gebruikers maar vooral meer geld voor de techreuzen. Het veranderen van dat verdienmodel zal helpen maar is niet voldoende. De honger naar data zit dieper dan dat. Een meer fundamentele aanpak is nodig. Een aanpak die ook oog heeft voor de mediamacht en marktmacht van bedrijven.

Hoe overheden met hun controlezucht steeds machtiger worden

“

The way the camera follows us in slo-mo

Boy in the bubble - Paul Simon

”

Een digitale dubbelrol: controlestaat en marktcontroleur

Als bedrijven te machtig zijn en de burger daar nadeel van ondervindt, dan is de overheid de aangewezen partij om de burger daartegen te beschermen. Dat is al niet gemakkelijk vanwege het grens overstijgende en complexe karakter van digitale technologieën en datastromen alsmede het private eigendom van de digitale infrastructuur. Maar afgezien daarvan is er een fundamenteeler probleem. Namelijk dat de overheid zelf uit controle-overwegingen ook een grote datagebruiker is en daarbij zelfs gebruik maakt van het bedrijfsleven. De overheid speelt dus een dubieuze dubbelrol als controlestaat en marktcontroleur.

De datazucht van de overheid

De digitalisering van ons dagelijks leven en de manier waarop steeds meer onderdelen van ons dagelijks leven gevat worden in data heeft ook gevolgen voor de machtsverhouding tussen overheden en mensen. Overheden verzamelen, koppelen en analyseren steeds meer data.

Bestaande databases van informatie over mensen zijn de afgelopen decennia gedigitaliseerd. Identiteitsgegevens, belastinggegevens, NAW-gegevens, adresgegevens, arbeidsgegevens, onderwijsgegevens, politie-databases, KvK-gegevens, passagiersgegevens van vluchten, enzovoorts. In totaal heeft de overheid meer dan 5000 databases met persoonsgegevens en zit de gemiddelde Nederlander in tientallen van dergelijke databases.³⁰ Tegelijkertijd gebruikt de politie ook steeds vaker private databases. Denk aan databases van bel- en internetbedrijven die bijhouden met wie je contact hebt, of aan locatiegegevens en data verkregen via social media.

Daarnaast zien we dat de overheid naast het digitaliseren van bestaande databases en het aanboren van private databases nog meer data over mensen verzamelt door middel van op internet aangesloten apparaten en andere nieuwe technologieën. Denk aan ANPR-camera's boven snelwegen, geluidssensoren, camera's in binnensteden, scanauto's voor parkeercontroles, en bodycams. Ook de wildgroei aan *smart city* initiatieven – projecten waarbij hele steden volgehangen worden met sensoren – worden hierbij gebruikt. Zelfs satellieten worden voor dit doel ingezet.³¹

Hiermee hebben overheden een completer overzicht van ons leven dan welke overheid in de geschiedenis van de mensheid dan ook, inclusief de autoritaire regimes van de 20e eeuw. En daarmee verschuift de machtsbalans tussen mens en overheid richting de overheid.

Maar de overheid verzamelt niet alleen meer data, het koppelt en analyseert ook steeds meer data. Een database geeft maar een klein beeld van iemands leven. Twee of drie gekoppelde databases leveren al een completer beeld op, laat staan als tientallen databases gekoppeld worden. Zo kan de overheid onder meer een beeld krijgen van waar je je bevindt, met wie je contact hebt en waar je je geld aan uitgeeft. Een completer beeld van iemands leven kun je je nauwelijks voorstellen.

De surveillancestaat: van SyRI en smart cities tot het Sociale kredietsysteem

Een voorbeeld van hoe dit nu gebruikt wordt is SyRI, oftewel Systeem Risico Indicatie. Dit is een systeem van de Rijksoverheid dat verschillende databases met persoonsgegevens aan elkaar koppelt om fraude op te sporen. De data van meer dan tien verschillende databases wordt gekoppeld. Een computer krijgt voorbeelden van bekende fraudeurs te zien en probeert op basis van die data verbanden te herkennen in de data van onschuldige mensen. Er bestaat op dat moment nog geen concrete verdenking. De data van onschuldige mensen wordt verzameld, gekoppeld en geanalyseerd om te kijken of ze iets fout gedaan hebben.

Waar leidt dit toe? De verbanden tussen bekende fraudeurs en de data van onschuldige mensen moeten worden gelegd door algoritmes die door mensen worden gemaakt. Het probleem is dat niemand die algoritmes mag inzien, evenals de data waarmee de algoritmes zijn getraind. Kortom, we hebben te maken met een klassieke *black box*. Het zou bij wijze van spreken kunnen dat het algoritme getraind is met data van alleen maar fraudeurs die op een oneven straatnummer wonen, waardoor het algoritme concludeert dat mensen op een oneven straatnummer eerder fraudeurs zijn. Door bias die zowel *data-based* (oude data, eenzijdige data, statistisch ongeldige data) als *rule-based* (algoritmes gebaseerd op onjuiste aannamen) kan zijn, liggen discriminatie en willekeur op de loer.

Het recht op privacy en de onschuldpresumptie zijn twee van de meest fundamentele kernwaarden van onze samenleving. Het recht op privacy houdt in dat een overheid niet zomaar in jouw privéleven mag rondneuzen en de onschuldpresumptie betekent dat je onschuldig bent tot het tegendeel bewezen is. Samen beschermen deze twee basisprincipes van onze rechtstaat mensen tegen discriminatie, willekeur en onderdrukking. Ze beschermen tegen een te machtige staat die de vrijheid van mensen beperkt.

Artikel 8 lid 2 van het Europees Verdrag voor de Rechten van de Mens zegt duidelijk: *“Geen inmenging van enig openbaar gezag is toegestaan in de uitoefening van dit recht, dan voor zover bij de wet is voorzien en in een democratische samenleving noodzakelijk is in het belang van de nationale veiligheid, de openbare veiligheid of het economisch welzijn van het land, het voorkomen van wanordelijkheden en strafbare feiten, de bescherming van de gezondheid of de goede zeden of voor de bescherming van de rechten en vrijheden van anderen.”*

Kortom, er is een zorgvuldige balans nodig tussen het recht op privacy, de openbare veiligheid en het economisch welzijn van het land. Het voorbeeld van SyRI markeert een punt in een verkeerde trend die de balans doet doorslaan. Daarmee slaan we een weg in die onze rechtstaat uitholt en uiteindelijk doodloopt.

Deze technologie staat namelijk allesbehalve stil. Opslag en rekenkracht van computers worden steeds groter en sneller, sensoren en camera's worden steeds beter en kunstmatige intelligentie wordt steeds geavanceerder. Dit leidt weer tot nieuwe toepassingen, zoals gezichtsherkenning, die gebruikt kunnen worden om mensen in real time te identificeren.

Waar kan dit allemaal toe leiden? China geeft het duistere voorbeeld. De Chinese overheid is druk bezig een systeem te implementeren dat mensen een 'social credit score' geeft. Data van bedrijven en overheden worden gekoppeld om een beeld te krijgen van mensen en in hoeverre zij goede onderdanen zijn. Slecht gedrag – het te laat betalen van boetes, door rood rijden, vrienden zijn met mensen met een lage score, te lang gamen – levert minpunten op. Goed gedrag – netjes je rekeningen betalen, kinderen krijgen, vrienden hebben met een goeie score – zorgt voor pluspunten. Camera's met gezichtsherkenning zorgen voor handhaving door mensen *real life* te identificeren en fout gedrag zoals door rood rijden te herkennen. Alles wat je doet wordt constant in de gaten gehouden, geanalyseerd en beoordeeld. Dit is de griezelige impact van digitalisering en datafificatie ten voeten uit.

Maar ook in democratische rechtstaten die vrijheid hoog in het vaandel hebben kan surveillance doorslaan. Neem de onthullingen van klokkenluider Snowden. De Amerikaanse inlichtingen- en veiligheidsdiensten hebben digitale technologieën gebruikt om gegevens te verzamelen over honderden miljoenen onschuldige mensen om ze te in de gaten te kunnen houden. Telefoongesprekken werden opgeslagen, internetverkeer werd wereldwijd afgetapt en consumentenapparaten werden gehackt.

Maar ook in Nederland zien we dat onze straten, wijken en steden volgehangen worden met camera's en sensoren, dat onze levens gevat worden in data en dat die data verzameld, gekoppeld en geanalyseerd wordt. De politie heeft een databank van 1,3 miljoen foto's.³² Scanauto's voor parkeercontrole worden ingezet voor alternatieve doeleinden.³³ De politie gebruikt software die misdaad voorspelt om de inzet van agenten te sturen³⁴ en maakt misbruik van camera's die voor andere doeleinden zijn opgehangen.³⁵ Ook krijgen inlichtingen- en veiligheidsdiensten en opsporingsdiensten steeds meer bevoegdheden om data te verzamelen, apparaten te kunnen hacken en data te analyseren.³⁶ Overal ter wereld zijn er steeds weer politici die encryptie (versleuteling) willen verzwakken waardoor mensen en bedrijven niet meer veilig en privé kunnen communiceren en beleidsmakers die nog makkelijker data van onschuldige mensen willen koppelen en analyseren.

Na 'Ik heb niets te verbergen' en 'Wie veilig wil zijn moet maar wat privacy inleveren' is 'Privacy is het schild van criminelen' het nieuwe motto van de techno-utopisten van de overheid. Zoveel verschilt die benadering niet van de techno-utopisten van de techreuzen, accuraat samengevat in de roman *The Circle* als *'sharing is caring and privacy is theft'*. Zij bekijken de wereld uitsluitend vanuit veiligheidsoptiek. Het zijn hamers en alles wat ze zien is een spijker. 'Privacy is het schild van criminelen' is een totalitaire uitspraak, er is geen nuance mogelijk. Mensen moeten al hun data delen met de overheid anders helpen ze criminelen.

Het leidt tot een samenleving zonder vrijheid en is volledig in strijd met de vrije, democratische rechtstaat die Nederland is.

Waar behoefte aan is, is een overheid die opstaat tegen de datamacht van techreuzen om haar burgers te beschermen door bij te sturen waar mogelijk en te begrenzen waar nodig. Maar haast het omgekeerde gebeurt. Langzaam maar zeker ontkomt ook de Nederlandse samenleving niet aan de praktijk van overheersende surveillance door de overheid. Een gevoel waarbij toezicht de overhand heeft: alles wat je doet wordt vastgelegd en bekeken. Een gevoel van onvrijheid die mensen belemmert zichzelf te zijn, zichzelf te ontplooien en daadwerkelijk vrij te zijn.

Het gaat langzaam maar zeker de verkeerde kant op. Maar het is nog niet te laat om het tij te keren. Maar dan moeten we wel nu beginnen.

Hoe we de macht terugbrengen bij mensen. Tijd voor een digitale revolutie

“

These are the days of miracle and wonder,
This is the long distance call.

Boy in the bubble - Paul Simon

”

De verwondering voorbij

De tijden van wonderen en verwondering waar Paul Simon in 1986 over zong zijn al lang en breed aangebroken. Het is ongelooflijk wat er allemaal mogelijk is met digitale technologie. Zelfrijdende auto's die ons van A naar B brengen, 3D-printers die voedsel printen, de creatieve en levensechte games die ons veel plezier brengen, salto springende robots en de mogelijkheid om afstanden tussen mensen letterlijk en figuurlijk te verkleinen. Nederland profiteert van- en draagt bovendien vol bij aan deze ontwikkelingen met bedrijven als Adyen, The Next Web, Booking.com, Hackerone, Elastic, ASML en Phillips.

In potentie biedt digitalisering een enorme kans om de vrijheid van mensen te vergroten, om mensen dichter bij elkaar te brengen, om mensen uit de armoede te tillen, om mensen veiliger te maken. Het geeft mensen de mogelijkheid om nieuwe bronnen van informatie aan te boren, om nieuwe passies en lotgenoten te vinden. Het heeft de potentie om kansgelijkheid te vergroten door informatie en kennis voor iedereen bereikbaar te maken. Gratis initiatieven als CodeAcademy maken het voor iedereen mogelijk om te leren coderen, een baan te vinden en zich omhoog te werken op de maatschappelijke ladder.

Dit is de belofte van digitalisering die we uit het oog zijn verloren. We dachten dat die ontwikkeling vanzelf zou komen. We zijn vergeten dat technologie niet automatisch onze waarden bevordert. We zijn vergeten dat mensen technologie maken en dat mensen technologie zo moeten vormgeven dat de waarden die we koesteren bewaakt in plaats van uitgehold worden. We zijn vergeten dat we moeten vechten voor onze vrijheid, onze democratie en onze rechtstaat.

We waren blind voor het sluipende mechanisme dat bedrijven en overheden machtiger zou maken en mensen afhankelijker zou maken. Met als gevolg: minder vrijheid, aantasting van onze democratie en uitholling van onze grondrechten. Dit is geleidelijk verlopen en daarom pas achteraf waarneembaar.³⁷ Het is tijd dat wij, mensen, die macht weer teruggrijpen. Het is tijd voor een digitale revolutie. Tijd voor een nieuwe scheiding der machten in het digitale tijdperk. Het is nog niet te laat. Mits we concrete stappen zetten om die macht terug te grijpen.

Cruciale randvoorwaarden, uitgangspunten en principes voor de digitale eeuw

Het bovenstaande heeft laten zien dat digitale technologieën een veelkoppig monster vormen dat verschillende fundamenteën van onze maatschappij onder vuur neemt. Dit vergt een brede en samenhangende aanpak op verschillende niveaus. Alvorens we ingaan op een aantal concrete voorstellen en maatregelen gericht op zowel bedrijven als overheden, schetsen we een aantal centrale uitgangspunten waaraan een duurzame digitale aanpak moet voldoen.

Allereerst moet de mens centraal staan. Menselijke waarden, ethische principes en burgerrechten dienen altijd leidend te zijn bij de ontwikkeling en toepassing van digitale technologieën.³⁸ Hierbij moet gedacht worden aan transparantie, aanspreekbaarheid, uitlegbaarheid, diversiteit, eerlijkheid en gelijkheid. Ten tweede moet sprake zijn van een mondiale en Europese aanpak. Gezien het grensoverschrijdende karakter van digitalisering zijn nationale oplossingen zelden zinvol. Internationale en intergouvernementele samenwerking is noodzakelijk. Ten derde moet de oplossing bij de bron (data) en bij het ontwerp (*by design*) beginnen. Vooraf nadenken dus. Achteraf moet er onafhankelijk toezicht zijn om onwenselijke en oneerlijke uitkomsten te herstellen. Ten vierde moeten bedrijven en overheden continu investeren in onderwijs en onderzoek. Een hoog kennisniveau en voldoende innovatiekracht zijn onmisbaar voor een leefbare digitale samenleving.

Bedrijven die menselijke waarden respecteren: minder datamacht, mediamacht & marktmacht

Het is hoog tijd om de datamacht die bedrijven over ons hebben in te perken door de hoeveelheid beschikbare data terug te dringen. De nieuwe Europese privacywet (AVG) is hierin een belangrijk onderdeel. Hoewel persoonlijke data met deze wet nog geen formeel eigendom van de gebruiker zijn, geeft deze wet mensen wel controle over data die bedrijven over hen hebben. Mensen mogen hun persoonsgegevens inzien, wijzigen en verwijderen. Sommige bedrijven nemen hierin ook al hun verantwoordelijkheid. Zoals Google dat mensen via privacy instellingen de mogelijkheid geeft het verzamelen van data en het tonen van gepersonaliseerde advertenties uit te zetten.

Maar er is meer nodig. De AVG zorgt er ook voor dat mensen toestemming moeten geven voor het delen van hun gegevens. Concreet betekent dit dat websites, apps en browsers niet de toegang mogen ontzeggen aan mensen die hun data niet willen afstaan. Bovendien moeten de cookiemuren en de app- en browserinstellingen standaard ingesteld staan op het niet verzamelen van data. In de praktijk is dit nog vrijwel nergens het geval, al die websites, apps en browsers zijn in strijd met de privacywet. De toezichthouder, de Autoriteit Persoonsgegevens, moet daarom streng toezicht houden en voldoende

middelen hebben om haar werk goed te kunnen doen. Momenteel beschikt de toezichthouder over te weinig middelen en menskracht.³⁹

Het inperken van de mediamacht van bedrijven is ingewikkelder. Bedrijven als Facebook, Twitter en Google hebben altijd volgehouden dat zij slechts neutrale doorgeefluiken van informatie zijn. Zij zien zichzelf niet als 'gatekeepers' van informatie, maar zijn dat feitelijk wel. Via algoritmes worden namelijk actief keuzes gemaakt om mensen bepaalde informatie en nieuws te laten zien. Het zijn poortwachters, maar ze nemen niet de verantwoordelijkheid die traditionele media wel op zich nemen. Het wordt tijd dat deze bedrijven dat wel gaan doen om zo de ergste uitwassen van desinformatie en manipulatie tegen te gaan. Dat zal geen gemakkelijke opgave zijn, want het gaat om de vrijheid van meningsuiting. Net als privacy is dat grondrecht niet absoluut en staat niks transparante en goed onderbouwde ingrepen van social media bedrijven in de weg. Bovendien is er een model dat deze bedrijven kunnen volgen, namelijk dat van traditionele mediaorganisaties. Deze hebben veelal een redactie (en vaak zelfs een ombudsman) die onafhankelijk van adverteerders bepaalt wat mensen te zien krijgen. Bij Facebook wordt wat mensen te zien krijgen 1 op 1 bepaald door wat het meeste geld oplevert. Er moet dus ook bij techreuzen een onafhankelijke redactie komen die bepaalt welke keuzes er gemaakt worden in het algoritme dat bepaalt wat mensen zien. Daarnaast hebben mediaorganisaties statuten waarin de journalistieke uitgangspunten op een transparante manier opgeschreven staan. Dergelijke transparantie over de uitgangspunten die ten grondslag liggen aan de inrichting van de algoritmes van Facebook, Google en Twitter is essentieel.

Daarnaast moeten afspraken gemaakt worden met bedrijven als Facebook, Google en Twitter die voor een groot deel het bezoekersaantal, en daarmee de inkomsten, van nieuwsmedia bepalen. De aftakeling van de landelijke en regionale journalistiek is een zorgelijke ontwikkeling in onze democratie. De journalistiek moet gehoord worden wanneer bedrijven als Facebook wijzigingen in algoritmes doorvoeren met grote invloed op de journalistiek.

Hoe? Bedrijven als Google en Facebook die een grote invloed hebben op de journalistiek en de manier waarop mensen nieuws tot zich nemen moeten een speciale aanmerking krijgen tot 'vitaal maatschappelijk bedrijf'. Deze aanmerking moet bedrijven dwingen tot het nemen van concrete maatregelen om het belang van journalistiek mee te nemen in belangrijke besluiten die van invloed zijn op de journalistiek. Bijvoorbeeld door een dialoog te starten met vertegenwoordigers van media om algoritmische keuzes te bespreken en daarover open te communiceren. Zo kunnen we grote techreuzen dwingen hun verantwoordelijkheid te nemen en de mediamacht van bedrijven terug te geven aan mensen.

De marktmacht van de grote industrialisten van de 20ste eeuw is met de uitvinding van het mededingingsrecht en mededingingsautoriteiten doorbroken. Die spelregels moeten we nu vertalen naar de digitale wereld om misbruik van economische macht door grote techreuzen te stoppen.

Ten eerste moet de optie bestaan om techreuzen te splitsen. Facebook, Google en Apple bieden een grote verscheidenheid aan diensten aan. Zo'n combinatie is gevaarlijk voor de economie en de democratie. Verschillende diensten van een enkel bedrijf kunnen namelijk moeiteloos data uitwisselen. En als poortwachter bepalen ze wie toegang heeft tegen welke prijs. In Duitsland is Facebook bijvoorbeeld al verboden om data van Duitse burgers uit Facebook, WhatsApp en Instagram te combineren.

Op Europees niveau kunnen lidstaten gezamenlijk een sterke vuist maken tegen dit soort praktijken.

Miljarden mensen maken gebruik van WhatsApp en Facebook betaalde voor de overname 21.8 miljard dollar. De toezichthouders konden niet eens een onderzoek opstarten, omdat WhatsApp gratis is en daarom nauwelijks omzet maakt. Een ouderwetse regel, waar je als consument de nadelen van ondervindt. Toezichthouders moeten zich niet blindstaren op de omzet. Ze moeten hun ogen open houden voor de overnamewaarde, de combinatie van data en netwerkeffecten. De onafhankelijke mededingingsautoriteiten, in Nederland de Autoriteit Consument & Markt (ACM), moeten een gezonde tegenmacht kunnen vormen. Dit kan door fusies scherper te onderzoeken, daar voorwaarden aan te verbinden of door ze te verbieden.

Bovendien moeten opkomende techbedrijven een eerlijke kans krijgen. Hun marktmacht geeft techreuzen een voorsprong die niet door andere bedrijven in te halen is. Door techreuzen te verplichten om sommige data te delen, kunnen nieuwe bedrijven hun eigen algoritmes even slim maken. Ook moet het als klant makkelijk zijn om over te stappen van techbedrijf naar techbedrijf. Als je genoeg hebt van Amazon moet jouw persoonlijke informatie overgezet kunnen worden naar een Disney+ abonnement. Naast deze dataportabiliteit zijn nog twee andere voorwaarden nodig, namelijk interoperabiliteit en non-discriminatie. Dit betekent dat technische barrières worden weggenomen zodat alle aanbieders met hun diensten kunnen inbreken bij de dominante spelers. En dat diensten van concurrenten op het eigen platform niet worden benadeeld. Als je je vrienden mee kan nemen van Facebook naar een ander netwerk of als bedrijven hun eigen appstore op de iPhone kunnen zetten dan wordt meer concurrentie en minder marktmacht mogelijk.

Naast de verplichting van de AVG om standaardinstellingen van apps en websites op het niet delen van data in te stellen (*opt-in*) zijn dit de belangrijkste maatregelen om de datahonger van techreuzen tegen te gaan. Als meer data niet langer meer geld betekent en als meer data niet langer een dominante marktpositie oplevert kunnen we echt een fundamentele verandering teweegbrengen en kunnen we negatieve gevolgen voorkomen.

Overheden die burgerrechten bewaken en respecteren

Naast het terugdringen van de datamacht van bedrijven moeten we de digitale macht die overheden naar zich toe hebben getrokken weer terugpakken. Die macht is het gevolg van het steeds meer verzamelen, koppelen en analyseren van data.

Dat begint met het inzichtelijk maken van het verschuiven van die machtsbalans. We moeten weten hoeveel databases met persoonsgegevens de overheid precies heeft opgesteld, welke databases precies door welke overheidsorganisaties worden gekoppeld en op welke manier en met welk doeleinde er analyses worden uitgevoerd.

Daarnaast moeten duidelijke wettelijke uitgangspunten geformuleerd worden die de digitale surveillancepraktijk in lijn brengt met bestaande grondrechten. Zomaar databases met persoonlijke informatie van onschuldige mensen koppelen en analyseren, zoals SyRI doet, kan niet zomaar en op

grote schaal. Dit kan enkel en alleen als er een duidelijk en belangrijk doel aan ten grondslag ligt, zoals uiteengezet in artikel 8 van het Europees Verdrag van de Rechten van de Mens (EVRM). En mits het met (vooraf) weldoordachte en (achteraf) controleerbare methodes gebeurt, die de privacy van onschuldige mensen zo min mogelijk raken. In alle andere gevallen moet er een concrete verdenking van een individu zijn als de overheid die databases wil raadplegen. Hier moet een duidelijke richtlijn voor ontwikkeld worden. Alle toepassingen van algoritmes die door databases met data van onschuldige mensen spitten, zoals SyRI, moeten wettelijk ingekaderd en begrensd worden zodat de Tweede Kamer controle kan behouden. Zolang deze duidelijke kaders er nog niet zijn, dienen experimenten en toepassingen te worden stilgelegd.

Dat betekent ook dat ANPR-camera's niet zomaar informatie over alle auto's die langskomen mogen opslaan, maar alleen over kentekens die onderdeel zijn van onderzoek.⁴⁰ En dat nieuwe technologieën, zoals gezichtsherkenningcamera's niet zomaar mogen worden toegepast zonder breed maatschappelijke debat, duidelijke richtlijnen en wettelijke waarborgen. Dat geldt ook voor het gebruik van dergelijke camera's voor het identificeren van niet-strafbare zaken zoals 'verward' gedrag of het samenkomen van een groep mensen of het opslaan van informatie van iedereen die langsloopt. Ook hier geldt: eerst duidelijke kaders die de technologie begrenzen, dan pas gebruik in de praktijk.

Kun je door al die digitale controle en surveillance meer misdaden opsporen? Waarschijnlijk wel. Maar dat betekent niet dat we het moeten doen. Als de prijs van het toepassen van die technologie het opgeven van grondwettelijke rechten en het uithollen van de rechtstaat is, dan is die prijs te hoog. Technologie moet in balans zijn met al onze basiswaarden.

Ook moet er meer grip komen om de wildgroei aan algoritmes en digitale technologie bij de overheid terug te dringen. Elke gemeente, elk ministerie en elke overheidsorganisatie, zoals de politie of het OM, is bezig met smart city experimenten of pilots met kunstmatige intelligentie. Vaak gebeurt dit met weinig tot geen oog voor de negatieve gevolgen. Bovendien is het belangrijk dat de Rijksoverheid de algemene situatie bewaakt. Daarom moeten overheden de toepassing van sensortechnologie, zoals gezichtsherkenningcamera's, verplicht melden bij de minister voor rechtsbescherming. Het terugbrengen van de macht van de overheid op digitaal gebied is geen zwart/wit kwestie waarbij met een paar maatregelen alles is opgelost. Het is een kwestie van constant afwegen in hoeverre al die digitale technologieën samen leiden tot een situatie waarin er sprake is van een te grote praktijk van surveillance.

De minister voor rechtsbescherming moet hierin een controlerende rol krijgen, inclusief de doorzettingsmacht om sommige experimenten of praktische toepassingen van technologie te stoppen. Daarnaast moet er een algoritme autoriteit komen die het gebruik van algoritmes kan controleren op discriminatie of uitsluiting en deze kan terugdraaien. Ook moet er een meldplicht komen voor het gebruik van ingrijpende algoritmes, zowel bij de toezichthouder als bij de minister.

Tot slot moet de overheid het goede voorbeeld geven, bijvoorbeeld door middel van een gedegen afwegingsproces om onbekende software-kwetsbaarheden te melden aan de producent in plaats van ze heimelijk te bewaren voor eigen gebruik en door encryptie te waarborgen en geen achterdeurtjes in te bouwen om te kunnen hacken.

Tijd voor een Digitale Revolutie

De afgelopen decennia is onze samenleving vergaand gedigitaliseerd. Dat heeft ons veel gebracht, maar het heeft ook schade toegebracht. Aan onze democratie en aan de machtspositie, de vrijheid, en de rechtspositie van burgers. De echte prijs van de goedkope fossiele energie in de vorige eeuw zien we nu terug in de klimaatcrisis. Zo zullen we ook de echte prijs van de gratis diensten van techreuzen in de toekomst moeten dragen in de vorm van uitholling van onze vrije, democratische rechtstaat. Tenzij we nu ingrijpen.

De analyse over de grote risico's van digitalisering en datahonger van techreuzen wordt breed gedeeld onder techdeskundigen. Wat echter lange tijd ontbrak was een politieke vertaling van die analyse naar concrete voorstellen tot verandering. Daar komt wereldwijd verandering in met de Amerikaanse senator (en Democratische presidentskandidaat) Elizabeth Warren en de vice-voorzitter van de Europese Commissie Margrethe Vestager (met de portefeuille digitalisering en mededinging) als prominente voorbeelden. Dit pamflet is een eerste aanzet voor het debat in Nederland. Waarbij simpele oplossingen voor dit probleem helaas niet bestaan. Een maatschappij-brede visie is noodzakelijk.

Met de maatregelen die we in dit pamflet voorstellen wordt de macht terug gegeven aan mensen, en de macht van bedrijven en overheden beperkt. Dat is essentieel om de risico's van digitalisering het hoofd te bieden, maar bovenal om de ongekende kansen ten volste te kunnen benutten. Met deze maatregelen kan de belofte van digitale technologie om de vrijheid van mensen te vergroten realiteit worden. Wie gelooft in de positieve kracht van digitalisering wil juist de risico's aanpakken. Met deze maatregelen kunnen we de digitale revolutie concreet vormgeven, onze waarden in het digitale tijdperk beschermen en mensen meer vrijheid geven. Zo voorkomen we een techno-dystopie en komt een humaan digitaal tijdperk binnen bereik.

Bijlage: De belangrijkste maatregelen in het kort

Macht van overheden inperken:

- Maak een wettelijk kader voor het gebruik van digitale besluitvormingssystemen zoals SyRI (die databases met gegevens van onschuldige mensen koppelen en analyseren). Leg vast dat het enkel en alleen mag voor zwaarwegende doeleinden en met voldoende, doordachte garanties om de burgerrechten van onschuldige mensen te beschermen.
- Maak een centraal overzicht van het aantal databases en de mate van koppeling.
- Stel een Algoritme Autoriteit in en een meldplicht voor algoritmegebruik. Maak een centraal overzicht voor vergaande algoritmes en automatische besluitvorming. Op die manier kunnen de Tweede Kamer en toezichthouders hun controletaak beter uitvoeren.
- Verbied gezichtsherkenning en ingrijpende algoritmes tot er wetgeving en toezicht is.
- Stel een coördinerende minister in voor rechtsbescherming tegen te grote datasurveillance vanuit de overheid.

Macht van bedrijven inperken:

- Vergroot de bewustwording over digitalisering en dataficatie onder mensen en kleine bedrijven.
- Garandeer data-eigendom en data-zeggenschap. Zet daarom stappen naar echte dataportabiliteit.
- De Europese privacywet AVG moet optimaal benut en gehandhaafd worden. Cookiemuren zijn dus verboden en webinstellingen moeten standaard op het niet delen van data staan.
- Toezichthouders als de Autoriteit Persoonsgegevens (AP), het Commissariaat voor de Media en de Autoriteit Consument en Markt (ACM) moeten meer middelen krijgen om hun werk te perfectioneren.
- Bedrijven als Google en Facebook moeten hun maatschappelijke verantwoordelijkheid nemen. Dit betekent dat ze een onafhankelijke redactie moeten instellen en openbare statuten moeten opstellen die uiteenzetten hoe en waarom hun algoritmes keuzes maken.
- Bedrijven als Google en Facebook krijgen de aanmerking 'vitaal maatschappelijk bedrijf' en moeten maatregelen nemen om belangen van de journalistiek te betrekken in keuzes over hun algoritmes. Desinformatie en *deepfake* moeten ingeperkt worden zonder censuur te veroorzaken.
- Verdere maatregelen tegen misbruik van economische macht: techreuzen opbreken; fusies verbieden; algoritmes inzichtelijk maken; data-delen verplicht maken en interoperabiliteit afdwingen.

Eindnoten

- 1 <https://www.theguardian.com/technology/2012/feb/01/facebook-letter-mark-zuckerberg-text>.
- 2 De fysieke infrastructuur van het internet bestaande uit kabels, knooppunten, datacenters en servers bevindt zich grotendeels buiten het zicht van mensen. De achterliggende datastromen, computerkracht en algoritmes zijn voor de meeste mensen een blinde vlek. Deze complexiteit van digitale technologie maakt het bijvoorbeeld ook lastig om er in begrijpelijke taal over te communiceren. Het resultaat: steeds zien we pas achteraf hoe ingrijpend de gevolgen zijn.
- 3 In haar boek "The Big Nine" (2019) schrijft Amy Webb over de Amerikaanse en Chinese techreuzen en hun denkende machines. Ze spreekt van "G-MAFIA" (Google, Microsoft, Amazon, Facebook, IBM en Apple) en "BAT" (Baidu, Alibaba en Tencent).
- 4 Journalist Huib Modderkolk beschrijft in zijn boek "Het is oorlog maar niemand die het ziet" (2019) hoe we de controle over onze data zijn kwijtgeraakt: "Inlichtingendienst AIVD trekt hele webfora leeg, inclusief de gegevens van mensen die geen doelwit van de dienst zijn. En wat voor de geheime dienst geldt, geldt ook voor bedrijven en overheidsinstanties."
- 5 <https://foreignpolicy.com/2016/06/29/the-man-who-nailed-jello-to-the-wall-lu-wei-china-internet-czar-learns-how-to-tame-the-web/>.
- 6 Susskind (2019): "Future Politics".
- 7 Voor een goede uitleg van deepfake en de maatschappelijke risico's, zie het recente rapport van Jarno Duursma hierover: "Deepfake Technology. The Infocalypse" (2019). https://www.jarnoduursma.nl/wp-content/uploads/2019/09/Jarno-Duursma_-_Deepfake-Technologie-The-Infocalypse.pdf.
- 8 <https://www.theguardian.com/technology/2012/feb/01/facebook-letter-mark-zuckerberg-text>.
- 9 Dit vormde ook de start van regelgeving om de risico's te beperken. Van de eerste Europese privacy richtlijn uit 1995 tot de cookiewet en uiteindelijk de Algemene Verordening Gegevensbescherming.
- 10 <https://www.ad.nl/binnenland/webcamafperser-stopt-strijd-in-nederland-en-wil-naar-canada-voor-zelfmoord-amanda-a7b67fb3/>.
- 11 <https://www.vrt.be/vrtnws/nl/2018/07/25/man-veroordeeld-voor-gluren-met-webcam-11578707-zr6367>
- 12 <https://www.nu.nl/internet/4936847/cybercrime-kost-nederlandse-economie-jaarlijks-10-miljard.html>
- 13 Susskind beschrijft in zijn boek uitgebreid hoe technologie onze vrijheid inperkt door overheden die surveilleren en gedrag voorspellen en door techbedrijven die informatie filteren en algoritmes die onze keuzes beïnvloeden; hoe technologie onze democratie schaadt door desinformatie en *deepfake*, fragmentisering in *filterbubbles* en *echochambers* plus *hatespeech* door bots en trolls; hoe technologie ingrijpt op sociale rechtvaardigheid door data-exploitatie zonder toestemming, oneerlijke verdienmodellen en marktconcentratie alsmede het verkeerd behandelen en benadelen van minderheden door schijnneutraliteit, statistische fouten oftewel *bias* (in zowel data als algoritmes). Het is dan ook niet overdreven om te stellen dat elke eigentijdse politicus zijn boek gelezen zou moeten hebben.
- 14 Vanwege hun enorme omvang en macht worden techreuzen vaak gezien als een markt en zelfs een staat op zichzelf. De vergelijking met een markt is begrijpelijk, maar wij spreken liever van monopolie of monopsonie. De vergelijking met een staat is minder voor de hand liggend omdat techreuzen mensen geen inspraak bieden, commercieel zijn en tevens oncontroleerbaar. Evenmin zijn hun diensten nutsfuncties die genationaliseerd kunnen worden. De suggestie van Susskind om te spreken van economische spelers met politieke macht is goed bruikbaar.
- 15 Hiermee bouwen we voort op de Techvisie 2.0 die D66 begin 2019 lanceerde: <https://d66.nl/techvisie-2-0-een-politieke-agenda-voor-de-digitale-toekomst/>.
- 16 Tegenwoordig ook vaak het "chilling effect" genoemd.
- 17 Welkom in de waanzinnige wereld van de online advertentie industrie die draait om gepersonaliseerd adverteren. U kent deze wereld wellicht van termen als *targeting* en *targeting* maar verder heeft u waarschijnlijk geen idee van de invloed die dit op uw gedrag heeft.
- 18 Ook omdat de Amerikaanse overheid – in tegenstelling tot de Chinese Volkspartij – op grote afstand staat van de techreuzen, ze ruim baan geeft en op onderdelen zelfs afhankelijk van ze is.
- 19 https://guce.techcrunch.com/copyConsent?sessionId=3_cc-session_442f8f6b-089a-4513-810b-1a5341fbc213&inline=false&lang=nl-NL.
- 20 <https://www.vrt.be/vrtnws/nl/2018/05/16/google-werkt-samen-met-pentagon--en-niet-iedereen-is-daar-blij-m/>.
- 21 China heeft daartoe een aantal zaaitprogramma's als *One Belt, One Road* (de nieuwe Zijderoute) en *Made in China 2025*.
- 22 <https://nos.nl/nieuwsuur/artikel/2227440-big-brother-2-0-in-china-bepaalt-je-sociale-score-je-leven.html>
- 23 In de VS beschouwt men data als eigendom van bedrijven, in China als eigendom van de staat en in Europa als eigendom van het individu. Je zou respectievelijk kunnen spreken van surveillance kapitalisme, surveillance socialisme en surveillance liberalisme. Over de immense impact van surveillance heeft Shoshana Zuboff het boek "The Age of Surveillance Capitalisme" geschreven.
- 24 <https://d66.nl/europese-techvisie/>
- 25 De schrijver Yuval Harari stelt in zijn boek *Homo Deus* zelfs dat mensen zelf ook algoritmes zijn en dus zeer makkelijk stuurbaar en manipuleerbaar.
- 26 Daarbij zijn ook data, code en algoritmes niet neutraal. Of preciezer gezegd: ze zijn misschien wel neutraal maar daarmee zijn oneerlijk. Dit omdat ze bestaande –menselijke– aannames, vooringenomenheid en benadeling bevestigen en versterken. Zoals Susskind zegt: neutraal is altijd in het voordeel van de machthebbers, nooit van de minderheden en onderdrukten.
- 27 <https://www.newyorker.com/news/our-columnists/mark-zuckerberg-doesnt-know-what-the-first-amendment-is-for>
- 28 Economen spreken ook van het first-mover advantage en het *winner-takes-all-principle*. Het komt er steeds op neer dat de dominante partij met datamacht de beste algoritmes en daarmee de meest optimale dienst kan ontwikkelen. Dit geeft een zichzelf versterkend effect dat concurrenten zo goed als buitenspel zet. In de D66 initiatiefnota "Mededinging in de digitale economie" (2019) gaan we uitgebreider op deze principes in: <https://www.tweedekamer.nl/kamerstukken/detail?id=2019Z02054&did=2019D04620>.
- 29 In haar boek *The Big Nine* schetst Amy Webb ook hoe machtsconcentratie en consolidatie kunnen leiden tot sociale gevolgen als segregatie en polarisatie. Als de techreuzen hun dominante positie weten uit te breiden naar steeds meer markten, kunnen zogenaamde Google-, Apple- en Amazon-gezinnen ontstaan, die alles in hun *smarthome* afnemen van een enkele aanbieder.
- 30 <https://sargasso.nl/meer-dan-5000-databases-met-persoonsgegevens-bij-overheid/>
- 31 <https://www.security.nl/posting/486380/Overheid+verkent+gebruik+satellieten+voor+monitoring>
- 32 <https://www.security.nl/posting/617777/Politie+heeft+database+met+foto's+van+1%2C3+miljoen+mensen>
- 33 <https://nos.nl/nieuwsuur/artikel/2302813-opsporingsdiensten-ontdekken-nieuw-wapen-de-scanauto.html>
- 34 <https://nos.nl/artikel/2286848-overheid-gebruikt-op-grote-schaal-voorspellende-algoritmes-risico-op-discriminatie.html>
- 35 <https://www.rtrnieuws.nl/tech/artikel/4886461/politie-kon-jarenlang-onterecht-amsterdamse-cameras-bekijken>
- 36 Onder meer op basis van de wet computercriminaliteit III (cc3) en de wet op de inlichtingen- en veiligheidsdiensten (wiv). Hoewel deze wetten op verschillende onderdelen zijn bijgesteld en begrensd, is er nog geen goed kader voor het gebruik van onbekende software-kwaatsigheden door de overheid. Daarom heeft D66 eind 2018 een initiatiefwet gediend om dit te regelen: <https://nos.nl/artikel/2264338-strengere-regels-nodig-voor-hacks-door-overheid-via-zero-day-bugs.html>.
- 37 Amy Webb spreekt in dit verband van "papercuts": geen grote explosie van verandering maar een sluipend proces van kleine sneetjes die langzaam maar zeker steeds meer nadelen en beperkingen opleveren.
- 38 Voor een humane ontwikkeling van kunstmatige intelligentie zijn afgelopen jaren door verschillende beleidsmakers en wetenschappers kernwaarden en principes opgesteld. De belangrijkste zijn: de Asilomar AI Principles van het Future of Life Institute, opgericht door natuurkundige Max Tegmark; An Ethical Framework for a Good AI Society; en de EU High-Level Expert Group on Artificial Intelligence.
- 39 In een recent onderzoek naar de benodigde middelen zijn drie scenario's uitgewerkt, 'laag', 'middel' en 'hoog' toezichtsniveau. Met het huidige budget wordt zelfs het laagste toezichtsniveau niet gehaald. Dit onderwerp is te belangrijk om de Autoriteit Persoonsgegevens niet uit te rusten op het hoogste toezichtsniveau.
- 40 Dit principe heet doelbinding: data die worden verzameld voor een bepaald doel, dienen ook enkel en alleen voor dat doel te worden gebruikt. Een regel die maar al te vaak wordt geschonden.

Digitale technologieën hebben ons leven enorm verbeterd. Van wereldwijde communicatie tot het genezen van ziektes. Maar in de begintijd van het internet klonk een nog grotere belofte: internet zou de wereld openen, de mensheid verbinden, welvaart beter verdelen, democratieën versterken en individuen vrijer maken.

Als we die utopische bril afzetten en kritisch kijken naar de gevolgen van digitalisering, is er veel meer aan de hand dan de zichtbare kant van blinkende gadgets, fraaie platforms en handige apps. De digitale droom is niet uitgekomen. Sterker nog, de digitale droom verandert langzaam in een nachtmerrie. De datahonger van techreuzen en overheden leidt tot de vele privacyschandalen van Facebook, manipulatie van verkiezingen door bedrijven als Cambridge Analytica en de onthullingen van Snowden. Maar nog fundamenteler leidt het tot een verschuiving van macht die ons minder vrij maakt en onze democratische rechtstaat aantast.

Dit pamflet is geschreven om de digitale sluipmoordenaar te ontmaskeren; om mensen te waarschuwen voor de fundamentele verandering van onze samenleving, als gevolg van digitalisering. De invloed van digitalisering op onze samenleving is onder de streep vooralsnog positief. Maar als we haar niet voldoende afremmen, bijsturen en begrenzen slaat die balans de verkeerde kant op.

Niets minder dan onze vrije, democratische rechtstaat staat op het spel. Het is tijd voor een digitale revolutie. We moeten voorkomen dat tijden van verwondering en verbazing omslaan in tijden van catastrofes en vervreemding.