DATAMACHT EN TEGENKRACHT

Kathalijne Buitenweg

DATAMACHT EN TEGENKRACHT

Hoe we de macht over onze gegevens kunnen terugkrijgen

2021
DE BEZIGE BIJ
AMSTERDAM

Met medewerking van Richard Wouters
Omslagontwerp Jan van Zomeren
Omslagbeeld Getty Images
Foto auteur Frank Ruiter
Vormgeving binnenwerk Aard Bakker
Druk- en bindwerk Wilco, Meppel
ISBN 978 94 031 2521 3
NUR 320

debezigebij.nl

Bij de productie van dit boek is gebruikgemaakt van papier dat het keurmerk van de Forest Stewardship Council (FSC®) mag dragen. Bij dit papier is het zeker dat de productie niet tot bosvernietiging heeft geleid.

Voor mijn collega's

Soms zullen we meer risico, imperfectie, improvisatie en ondoelmatigheid moeten aanvaarden om de democratische geest levend te houden.

EVGENY MOROZOV

INHOUD

DATAMACHT

Ter inleiding

Het lijkt lichtjaren terug, maar tot 2011 was het Nederlandse Hyves groter dan Facebook, tot 2008 kon ik alleen maar bellen op mijn telefoon en mijn scriptie schreef ik op een enorme typemachine – met een potje Tipp-Ex bij de hand. Digitalisering heeft onze manier van werken in snel tempo veranderd. Daarmee groeide ook de hoopvolle verwachting dat nieuwe technologie onze wereld beter zou maken. Want hoe meer we weten, hoe meer we kunnen. En onderling verbonden staan we samen sterk.

In vol vertrouwen hebben we de afgelopen jaren steeds meer data afgestaan. Overheden maken daar gebruik van om inspraakprocedures te organiseren, diensten te verlenen en om beter te voorspellen wie van ons de wet zal overtreden of hulp nodig heeft. Bedrijven krijgen via onze gegevens meer zicht op onze diepste wensen en interesses, en stemmen daar hun nieuwsberichten en producten op af. Ook steeds meer werkgevers maken gebruik van

persoonsgegevens en andere data om de talenten, de valkuilen en het werkethos van hun medewerkers te meten. Allemaal reuze handig en *slim*, maar wiens belang dienen onze data nu eigenlijk? Na de jaren van hoop worden we steeds vaker geconfronteerd met de keerzijde van deze dataverzameldrift.

Bij de Belastingdienst blijken 180.000 mensen op een zwarte lijst te staan zonder dat duidelijk is waarom ze in dit bestand van mogelijke fraudeurs voorkomen. En omdat ze door het systeem collectief als risico zijn aangemerkt, werden mensen met een tweede nationaliteit anders behandeld dan mensen met alleen de Nederlandse nationaliteit. Zorgen zijn er ook over de gedetailleerde profielen die techbedrijven van ons maken. Op basis van onze aankopen, contactgegevens, zoektermen, locaties, berichten en *likes* leren bedrijven ons steeds beter 'kennen'. Dankzij al deze data wordt het niet alleen makkelijker om ons koopgedrag te manipuleren, maar zelfs onze keuze in het stemhokje. Waar we hoopten dat digitalisering de samenleving zou verbinden, dreigt het omgekeerde. Door gepersonaliseerde advertenties en nieuwsberichten ontstaan gescheiden werelden waarin mensen niet meer dezelfde informatie zien, lezen of horen.

Data vormen een bron van macht. Volgens de Wetenschappelijke Raad voor het Regeringsbeleid 'worden burgers steeds transparanter voor de overheid, terwijl de profielen, algoritmen en methoden die overheidsorganisaties gebruiken nauwelijks transparant of navolgbaar voor die burgers zijn'.[1] Hetzelfde geldt voor de profielen, algoritmes

en methoden van internetbedrijven en werkgevers. Veel keuzes worden niet door maar voor ons gemaakt, en we weten zelfs vaak niet op basis waarvan. Door digitalisering verschuift de macht met steeds grotere snelheid in de richting van bedrijven en overheden – weg van burgers, internetgebruikers en werknemers.

Het ongemak over het groeiende databezit van bedrijven en overheden neemt de laatste jaren weliswaar toe, maar dat leidt nog onvoldoende tot het organiseren van tegenmacht. Eerder wordt de oplossing gezocht in het verbeteren van systemen of in het afwentelen van de verantwoordelijkheid op burgers. Die moeten hun data maar beter beschermen, en minder makkelijk overdragen. Het doet denken aan de discussies over het klimaat. Ook daar werd lange tijd alles teruggebracht tot het niveau van individuele keuzes. Maar een beroep daarop volstaat niet om te komen tot noodzakelijke verandering. Temeer omdat de gevolgen van grootschalige overdracht van persoonsgegevens niet louter op het bordje komen van mensen die ervoor hebben gekozen om deze gegevens af te staan. Want in deze tijd van *big data* is het mogelijk om via het combineren van veel verschillende gegevens een meetlat te maken waarlangs iedereen wordt gelegd, inclusief de mensen die zelf geen gegevens hebben aangeleverd. Ook de impact van datatoepassingen gaat de individuele verantwoordelijkheid te boven en komt voor onze gezamenlijke rekening. Zo is Facebook, volgens voormalig topbestuurder Chamath Palihapitiya, hard op weg om het sociale weefsel van de samenleving te vernietigen. Met behulp van data

die het bedrijf via 'dopamineachtige beloningen voor de korte termijn' aftroggelt, ondergraaft 'het monster' een gezond maatschappelijk debat, en verspreidt het desinformatie en onwaarheden.[2] Dat is dus wat er op het spel staat: onze vrijheden en democratie.

Maar kúnnen we onze privacy nog wel beschermen? Het valt niet mee om het vertrouwen daarin overeind te houden nu er zo'n enorme dataverzameldrift is ontketend. Toch is dat de kern van dit boek. Mijn optimisme is oprecht, maar ook deels zelfopgelegd – vanuit de overtuiging dat fatalisme ons niks brengt. Want de Brits-Oostenrijkse filosoof Karl Popper had gelijk:

> De toekomst hangt af van wat wij doen. Wij dragen alle verantwoordelijkheid. Dus het is onze plicht, niet om het kwaad te voorspellen, maar om te vechten voor een betere wereld.[3]

In die betere wereld maken we wat mij betreft volop gebruik van technologische innovaties en geanonimiseerde data, maar beschermen we tegelijkertijd met veel meer kracht onze privacy, autonomie en een eerlijke economie. Volgens Google-directeur Matt Brittin is zo'n dubbele opdracht onmogelijk. In zijn ogen is het opkomen voor waarden als privacy antimodernistisch: 'een neiging om het verleden te beschermen tegen de toekomst'.[4] Maar zulke pogingen om het financiële eigenbelang te beschermen zijn opzichtig en steeds minder geloofwaardig. We zitten in een nieuwe fase – in lijn met de ontwikkelingen die Karl

Marx beschreef ten tijde van de eerste industriële revolutie:

> Er is tijd en ervaring nodig voordat de arbeider een onderscheid kan maken tussen de machine en haar kapitalistische toepassing, en dus zijn aanvallen kan richten, niet tegen de materiële productiemiddelen zelf, maar tegen de maatschappelijke vorm waarin deze productiemiddelen worden gebruikt.[5]

Dát had Marx in elk geval goed gezien. In de afgelopen jaren hebben we de tijd gehad om de digitale revolutie te doorgronden; we zijn steeds beter in staat om de technologie te onderscheiden van hoe die wordt toegepast en wiens macht zij vergroot. Het komt er nu op aan die kennis te gebruiken en grenzen te stellen aan het gebruik van technologie die onze samenleving niet dient. De duizelingwekkende snelheid waarmee technologische innovaties elkaar opvolgen, en het mondiale karakter daarvan, mogen ons daarbij niet verlammen, maar moeten ons juist aanmoedigen om niet langer te wachten.

In dit boek doe ik een aantal aanbevelingen om tegenmacht te organiseren. Om *Big Tech* te reguleren, om intimidatie en manipulatie via sociale media tegen te gaan, om werknemers meer zeggenschap te geven over de inzet van robots en het gebruik van hun data, om de transparantie van algoritmes te vergroten, om de handel in en met persoonsgegevens te verbieden, en nog veel meer. Het is een politie-

ke agenda die verre van compleet is, gestuurd wordt door mijn eigen ervaringen, en waar vast wat op af te dingen valt. Mijn belangrijkste doel is dat we kritischer worden op de talloze vormen van privacyschending die we bijna als normaal zijn gaan beschouwen, dat we ze erkennen als een bedreiging voor onze vrije samenleving, en dat we de moed vinden om voor onze democratische waarden te knokken.

In het eerste hoofdstuk ga ik dieper in op de waarde van privacy. Privacy is niet alleen een individueel recht, maar ook een publiek goed – en een voorwaarde voor het realiseren van andere vrijheden. In hoofdstuk twee bespreek ik de voorspellende profielen die de overheid hanteert en de gevolgen daarvan voor sociale ongelijkheid. Hoewel ze vaak tot doel hebben om de tweedeling aan te pakken, dreigt het tegenovergestelde. De vier daaropvolgende hoofdstukken hebben vooral betrekking op het gebruik van data door bedrijven. Het gaat om de handel in en met persoonsgegevens, het gebruik van data door werkgevers en de impact van sociale media. Omdat emancipatie van vrouwen de leidraad in mijn werkzame leven is, concentreert hoofdstuk vijf zich op de positieve en negatieve gevolgen van sociale media voor vrouwen. De voorstellen die ik in de verschillende hoofdstukken doe om tegenmacht te bieden, zullen vaak in Europees verband moeten worden verwezenlijkt. Daarom is hoofdstuk zeven gewijd aan de rol van de Europese Unie en het geopolitieke speelveld. Hoofdstuk acht ten slotte gaat in op de kansen en risico's van digitalisering voor vergroening en duurzaamheid. Waar digitale innovatie de potentie heeft om een enorme

bijdrage te leveren aan het tegengaan van klimaatverandering en de schaarste in grondstoffen, zien we in de praktijk dat veel nieuwe toepassingen juist leiden tot verdere uitputting van de aarde.

Sensoren en data, algoritmes en apps, digitale netwerken en platforms hebben ons leven in korte tijd ingrijpend veranderd, en vaak ten goede. Nog steeds biedt digitalisering ongekende mogelijkheden om onze wereld beter te maken: veiliger, democratischer, socialer en groener. Een wereld van gelijkere kansen.

Maar dat kan alleen als macht wordt begrensd door tegenmacht.

1 HET BELANG VAN PRIVACY

Waarom privacy een publiek goed is

Het belang van privacy is pakkend beschreven in *De Cirkel* van Dave Eggers. Ik kreeg het boek in de zomer van 2014 toegeschoven door mijn dochter, die het omschreef als haar ultieme nachtmerrie. Terwijl ik de dagen erna las over Mae Holland en haar leven als werknemer bij het machtigste techbedrijf ter wereld, een combinatie van Google en Facebook, bekroop me eenzelfde gevoel van horror. Maes bazen streven een wereld na waarin iedereen alles over elkaar mag weten onder het motto: 'Geheimen zijn leugens. Delen is mee-leven. Privacy is diefstal.'[1] Overtuigd van het belang van transparantie kiest Mae ervoor om permanent een camera mee te dragen waarvan de beelden 24 uur per dag voor iedereen te zien zijn. Ze hoopt dat vooral politici haar voorbeeld zullen volgen, want zonder privacy is er geen plek voor intriges en gekonkel en zal wereldvrede spoedig volgen.

Het angstaanjagende zit niet in het boek zelf, maar in

het besef dat ook in onze samenleving het idee langzamerhand heeft postgevat dat mensen met goede bedoelingen maar weinig privacy nodig hebben. Zoals Eric Schmidt, voormalig topman van Google, het ooit verwoordde:

> Als je iets doet waarvan je niet wilt dat anderen het weten, kun je het misschien beter maar helemaal niet doen.[2]

Maar een samenleving waar volledige transparantie heerst, is een onvrije samenleving. Als onze privacy niet wordt gerespecteerd, staan ook andere mensenrechten op de tocht, zoals het stemrecht en de vrije pers.

WETEN WE WEL WAT WE DELEN?

Wat is privacy eigenlijk, en wanneer wordt zij geschonden? Het is niet eenvoudig om daar antwoord op te geven. Veel hangt af van de situatie. Volgens de Amerikaanse filosofe Helen Nissenbaum ervaren we een inbreuk op onze privacy wanneer informatie over ons wordt gedeeld op een manier die niet overeenkomt met onze verwachtingen.[3] Zo verwachten we niet dat wat we bespreken met een arts in de spreekkamer door haar vervolgens wordt gedeeld met de buurvrouw. Dat zou een schending van privacy en vertrouwen zijn. Maar als je op het schoolplein vertelt dat je ernstig ziek bent, vind je het misschien niet gek als dit nieuws zijn weg vindt naar andere ouders – hoewel je

waarschijnlijk niet verwacht dat het bericht via Facebook de ronde doet. Of misschien ook weer wel wanneer je een publiek figuur bent. Kortom, privacy is afhankelijk van de context. Wat in de ene situatie oké is, is dat in een andere misschien niet. En wat de ene persoon aanvaardbaar vindt, geldt niet automatisch voor de andere. Daarom is het belangrijk dat mensen zelf kunnen bepalen welke gegevens ze delen en wat daarmee gebeurt.

Maar aan die zeggenschap schort het al enige tijd. Digitalisering heeft het mogelijk gemaakt dat onvoorstelbare hoeveelheden data over ons worden gegenereerd en vervolgens gedeeld voor heel veel verschillende doelen. Onderzoeksjournalisten Maurits Martijn en Dimitri Tokmetzis volgden gedurende drie jaar de digitale informatiestromen in ons dagelijks leven onder het motto: *follow the data.* In hun boek *Je hebt wél iets te verbergen* concluderen ze dat we de grip volledig kwijt zijn:

> We weten helemaal niet welke gegevens we allemaal weggeven. We hebben geen idee wie er – bevoegd of onbevoegd – toegang tot die data hebben. En we weten niet om welke redenen andere partijen in onze data geïnteresseerd zijn, wat ze ermee doen en welke beslissingen over ons worden genomen op basis van die data.[4]

Als gevolg daarvan worden onze gegevens gebruikt op manieren die we waarschijnlijk ongepast vinden – als we het zouden weten. Een bekend voorbeeld hiervan is de marketingmethode van de Amerikaanse winkelketen Target. De

statisticus van dienst, Andrew Pole, kreeg in 2002 de opdracht om beter inzicht te krijgen in het persoonlijk leven van klanten door klantendata te combineren. Het ging om veel verschillende gegevens waaronder leeftijd, inkomen, betaalgegevens, aankopen, huwelijkse staat, adres- en verhuisgegevens enzovoort. Pole slaagde erin om met behulp van deze vergaarbak een algoritme te ontwikkelen waarmee hij met vrij grote zekerheid kon berekenen welke klanten in een vroeg stadium van hun zwangerschap zaten. Vooral de aankoop van ongeparfumeerde zeep, in combinatie met voedingssupplementen als magnesium, zink en calcium, bleek een goede indicator voor aanstaand ouderschap. Target stuurde vervolgens de klanten die hoog scoorden op de waarschijnlijkheidsladder gerichte aanbiedingen, en hoopte zo de jonge moeders voor langere tijd aan zich te binden. Het verhaal gaat dat in 2011 een tiener uit Minneapolis coupons voor babykleertjes kreeg toegestuurd nog voordat haar ouders wisten van haar zwangerschap.[5]

Het voorbeeld laat zien dat gegevens die op zichzelf niet gevoelig zijn, in combinatie met andere data dat ineens wel kunnen worden. En ook al weten we dat Target bijhoudt welke aankopen we doen, dan verwachten we nog niet dat het bedrijf daaruit conclusies trekt over een eventuele zwangerschap, soms zelfs voordat we onze familie daarvan op de hoogte hebben kunnen stellen. Daarmee wordt het een inbreuk op privacy.

Een discussie over de ongepastheid van het gebruik van gegevens maakte ik ook mee in 2003 als lid van het Europees

Parlement. Toen ging het om informatie over vliegtuigpassagiers. In de nasleep van de aanslagen op 11 september 2001 eiste de Amerikaanse regering bovenmatig veel informatie op over iedereen die naar de Verenigde Staten vloog. Het ging veel verder dan het delen van de gebruikelijke identiteitsgegevens zoals naam en paspoortnummer. In een poging nieuwe aanslagen te voorkomen, legden de Amerikanen ook de hand op creditcardgegevens en zelfs maaltijdkeuzes. Naar alle waarschijnlijkheid wilden ze daar een geloof of levensovertuiging uit afleiden, om vervolgens te kunnen inschatten in hoeverre een reiziger een gevaar vormt voor de nationale veiligheid. De overdracht van zulke persoonsgegevens was destijds in strijd met de Europese privacywetgeving, en daarmee onrechtmatig. Maar de Europese Commissie, het dagelijks bestuur van de Europese Unie, en de nationale regeringen lieten het stilletjes gebeuren, uit angst voor economische repercussies. Reizigers werden zelfs niet geïnformeerd.

Om de stilte te doorbreken togen mijn Italiaanse collega Marco Cappato en ik, op initiatief van burgerrechtenorganisatie Bits of Freedom, op 20 mei naar vliegveld Zaventem. Om beurten stapten we op de passagiers af die in lange rijen voor de balie stonden en vroegen hen het hemd van het lijf. Wat het nummer was van hun creditcard, welke maaltijd ze hadden besteld, met wie ze reisden en nog veel meer. Mensen waren verbijsterd. Toen we uitlegden dat ze al deze informatie aan het eind van de rij ook zouden afstaan aan de Amerikaanse autoriteiten, ontstond er een levendige discussie. Sommigen vonden de overdracht van

maaltijdgegevens aanvaardbaar, gezien de dreiging van terrorisme. Anderen ging het veel te ver. Zij hadden er geen probleem mee gehad om bij het reisbureau kenbaar te maken dat ze koosjer, halal of vegetarisch wilden eten, maar dat deze informatie vervolgens gebruikt werd in de context van nationale veiligheid baarde ze zorgen. Want hoe zou er dan naar hen gekeken worden? Ze *ervoeren* het als een inbreuk op hun privacy.

In 2019 heeft de overdracht van passagiersgegevens vanuit Nederland naar de Verenigde Staten overigens alsnog een wettelijke basis gekregen. De maaltijdkeuzes zijn daarbij uitgezonderd. Want ook de wetgever vond dat uiteindelijk een brug te ver.

DATAVERZAMELDRIFT

Bij privacy gaat het niet alleen om subjectieve verwachtingen en ervaringen, maar ook om een recht. Een mensenrecht, vastgelegd in Europese en internationale verdragen en in artikel 10 van de Nederlandse Grondwet. Het eerste lid daarvan luidt:

> Ieder heeft, behoudens bij of krachtens de wet te stellen beperkingen, recht op eerbiediging van zijn persoonlijke levenssfeer.

Onder privacy valt onder meer het recht op eerbiediging van het innerlijk leven, het recht op zorgvuldige behan-

deling van persoonlijke gegevens en het recht om niet te worden bespied of afgeluisterd.

Privacy is geen absoluut recht. Het is aan de wetgever om te bepalen welke inbreuken gerechtvaardigd zijn. Die inbreuken moeten wel noodzakelijk, proportioneel en effectief zijn. Als de minister bijvoorbeeld overweegt om alle postpakketjes te openen om drugszendingen op het spoor te komen, dan zal zij duidelijk moeten maken dat het probleem echt heel ernstig is en dat hetzelfde resultaat niet bereikt kan worden op een minder ingrijpende manier – bijvoorbeeld door de inzet van drugshonden die gericht aangeven welke pakketjes aan een nader onderzoek moeten worden onderworpen. Dezelfde vereisten gelden voor digitale postpakketjes, of voor het gebruik van de persoonsgegevens die we achterlaten op internet. Het vergaren van persoonlijke informatie moet dus in lijn zijn met twee richtinggevende principes. Allereerst het principe van *dataminimalisatie*: er mogen niet méér gegevens worden verzameld dan nodig is om het doel te behalen. En ten tweede *doelbinding*: de gegevens mogen alleen worden gebruikt voor het doel waarvoor ze zijn verzameld. Deze principes zijn vastgelegd in onze privacywetgeving: de Algemene Verordening Gegevensbescherming (AVG). Het is een wet die in de hele Europese Unie op een uniforme manier wordt toegepast.

De afgelopen jaren hebben zich verschillende ontwikkelingen voorgedaan die het moeilijker maken om het recht op privacy overeind te houden. Laat ik beginnen met de technologische ontwikkelingen.

Digitale systemen worden steeds sneller en beter. Doordat het verzamelen, transporteren en opslaan van data goedkoper is geworden, en de rekenkracht van computers enorm is toegenomen, is het mogelijk om steeds meer gegevens te combineren en daar conclusies uit te trekken. Dat gaat aan de hand van algoritmes: beslissystemen of wiskundige formules die een gevolgtrekking afleiden uit de ingevoerde informatie ('als dit, dan dat'). Er bestaan ook algoritmes die zelflerend zijn. Daarbij past de computer niet simpelweg een formule toe die door mensen is ontwikkeld, maar verbetert de computer zelf de uitkomsten door die steeds weer te toetsen met behulp van nieuwe data en zo te leren van voorbeelden.

Algoritmes die worden gevoerd met veel verschillende gegevens kunnen tot onverwachte inzichten komen, zoals het voorbeeld van winkelketen Target liet zien. Ineens bleek het mogelijk om de statistische waarschijnlijkheid van een zwangerschap van klanten te berekenen. Hoe meer data uit verschillende bronnen worden ingevoerd, hoe meer statistische verbanden kunnen worden blootgelegd. Wellicht dat het bedrijf in de toekomst, via goed combineren en analyseren, zelfs een kansberekening kan maken van de seksuele gerichtheid van de jonge moeders, en daarmee potentiële klanten kan rekruteren voor een cursus 'roze ouderschap'.

Het oude adagium *select before you collect*, waarbij alleen die gegevens verzameld worden die nodig zijn om het doel te bereiken, wordt bedreigd door een nieuw credo: *collect before you select*. Daarbij worden eerst zoveel mogelijk gegevens binnengeharkt, om daarna pas te kijken wat

ermee mogelijk is. Ondanks de wettelijke verplichting tot dataminimalisatie en doelbinding blijken in de praktijk de technologische mogelijkheden onweerstaanbaar.

Het zijn niet alleen commerciële partijen die de randen van de privacywetgeving opzoeken. Ook overheden zwichten voor de verleiding van *function creep*, oftewel het voor andere doelen gebruiken van informatie dan waarvoor die is verzameld. Denk aan de camera's boven de snelweg: die zijn opgehangen om te registreren wie te hard rijdt, en om deze chauffeurs te kunnen beboeten. Maar toen de camera's er eenmaal waren, werd het aantrekkelijk om ze ook in te zetten voor een ander doel, namelijk het opsporen van gestolen auto's. Zodra een kans zich aandient, vergt het blijkbaar veel zelfbeheersing om die niet te grijpen.

Met de toename van digitale toepassingen is function creep steeds normaler geworden. De lat voor het schenden van privacy wordt in de praktijk steeds lager gelegd: van 'noodzakelijk' naar het niveau van 'best handig' en 'wie weet levert het wat op'. Volgens de Wetenschappelijke Raad voor het Regeringsbeleid wordt de maatschappelijke impact van het gebruiken van gegevens voor steeds meer doelen onvoldoende doordacht:

> Function creep gaat in de regel in kleine incrementele stapjes: er wordt een koppeling gemaakt tussen het ene en het andere systeem, er komt toegang voor een nieuwe organisatie tot deze data, enzovoort. Voor elk van deze stapjes is op dat specifieke moment een po-

litieke rechtvaardiging te geven – effectievere, betere dienstverlening, veiliger – maar het cumulatieve resultaat is vaak veel groter dan de som der delen. Bovendien is het 'eindresultaat' iets waar nooit een serieus politiek debat over is gevoerd.[6]

De steeds grotere mogelijkheden van computers hebben ook gevolgen voor de omgang met gevoelige gegevens, zoals informatie over gezondheid, seksuele gerichtheid, ras en levensovertuiging. Met slechts een beperkt aantal uitzonderingen daarop, is het verboden om deze gegevens te verzamelen en op te slaan. Maar de grens tussen de categorieën gegevens begint langzaam te vervagen omdat het nu mogelijk is om grote hoeveelheden gegevens die op zichzelf niet gevoelig zijn, en die verzameld mógen worden, te combineren en op die manier conclusies te trekken die wél gevoelig zijn. Uit recent onderzoek van de Noorse consumentenbond blijkt dat er al bedrijven zijn die zo de seksuele gerichtheid van iemand achterhalen, en die informatie gebruiken om gericht te adverteren.[7] Technologische ontwikkelingen ondergraven op deze manier wat de wet wil voorkomen: dat onze persoonlijke levenssfeer in het geding komt.

VEILIGHEID VOOROP

Privacy is de afgelopen jaren niet alleen door technologische, maar ook door maatschappelijke veranderingen

onder druk komen te staan vanuit een grotere drang naar controle en veiligheid. Volgens de Duitse socioloog Ulrich Beck, die in 1986 het begrip 'risicomaatschappij' muntte, hebben mensen in westerse samenlevingen in toenemende mate moeite om goed om te gaan met ongeluk en tegenslag. Er heerst een beeld dat mensen zelf verantwoordelijk zijn voor hun geluk en succes, en dus ook voor hun ongeluk en falen. Het idee dat we ons leven in eigen hand hebben, maakt dat we ons willen indekken tegen tegenslag. Daarvoor kijken we al snel naar de staat. We eisen van de overheid gegarandeerde veiligheid: in het verkeer, op straat, in de speeltuin, op het werk. Sinds 9/11 staat veiligheid nóg prominenter op de politieke agenda. Een terroristische aanslag is zó angstaanjagend en destabiliserend dat het voorkomen daarvan de grootste prioriteit van de overheid is geworden. Voor het wegnemen van concrete dreigingen, of volgens terrorismedeskundige Beatrice de Graaf zelfs 'het voorkomen van risico's überhaupt', zijn we bereid veel te accepteren.[8] We hunkeren naar een risicoloze samenleving.

De hang naar honderd procent veiligheid sluit naadloos aan bij een wens die overheden al van oudsher hebben: maximale rust en orde. Als onrust onder burgers tijdig wordt ontdekt en opstanden voorkomen, dan blijven de machtsverhoudingen in stand.[9] De controledrift van de overheid is met de eeuwen alleen maar sterker geworden en nu is er bovendien de techniek om die controle handen en voeten te geven. Mensen worden letterlijk 'leesbaar' gemaakt doordat er steeds meer informatie over hen wordt

verzameld en gecombineerd. Met behulp van algoritmes worden ze vervolgens in categorieën ingedeeld voor overheidsaandacht op maat.

Of dat ook betekent dat de samenleving inderdaad veiliger wordt, is nog de vraag, maar aan die vraag komen veel beleidsmakers en politici nauwelijks toe. Volgens de Wit-Russische publicist Evgeny Morozov wordt alles wat op het gebied van veiligheid technisch mogelijk is, al snel gezien als wenselijk. Maar:

> Daarbij wordt vaak vergeten om goed te onderzoeken of de toepassing ook inderdaad effectief is. Er is een overdreven vertrouwen in technologie, en een neiging om voor problemen geen andere oplossing te zien dan 'digitale pleisters'.[10]

Er heerst een overdreven techno-optimisme. Exemplarisch is de behandeling in de Tweede Kamer van de 'Wet gebruik van passagiersgegevens voor de bestrijding van terroristische en ernstige misdrijven' om de eerdergenoemde overdracht van informatie over vliegtuigpassagiers aan de Verenigde Staten formeel te regelen. Uit onderzoek blijkt dat juist bij terrorismebestrijding het verzamelen van zoveel mogelijk informatie over iedereen minder effectief is dan investeren in gerichte opsporing. Het is namelijk buitengewoon lastig om een goed profiel van potentiële daders op te stellen. Anders dan inbraken, komen terroristische aanslagen weinig voor en varieert ook de manier waarop ze gepleegd worden te veel om daaruit voorspellende conclusies

te kunnen trekken.[11] In de toelichting bij het wetsvoorstel gaf de regering toe dat zij niet aannemelijk kon maken dat het verzamelen van alle gevraagde data nuttig en noodzakelijk was. Toch is de wet aangenomen. Dat is deels te verklaren door de druk van de Amerikanen, deels door een te groot vertrouwen in technologische oplossingen, maar ook door de angst die veel politici voelen, dat hen achteraf iets te verwijten valt. Om vooral geen risico's te nemen met onze nationale veiligheid, tasten we zo onze vrijheid aan.

Zorgen over privacy worden vaak met gemakzuchtige dooddoeners terzijde geschoven. Neem voormalig minister van Justitie Ivo Opstelten. Als burgemeester van Rotterdam voerde hij campagne met de leus: 'Ik vind dat veiligheid boven privacy gaat.' Daarmee suggereerde hij dat het om een simpele uitruil gaat, waarbij meer privacy leidt tot minder veiligheid en andersom. Maar zo simpel is het niet. Privacy is juist van groot belang om onze veiligheid te waarborgen. Niet voor niets stak er een storm van verontwaardiging op toen begin 2021 bekend werd dat medewerkers van de GGD persoonsgegevens hadden ontvreemd uit een database van miljoenen mensen die op corona waren getest, om ze vervolgens door te verkopen aan cybercriminelen.

Een betere bescherming van onze privacy verdient prioriteit. Cybercrime is de snelst groeiende vorm van criminaliteit. Het gaat dan vaak om betaalfraude, zoals phishing, of om chantage van burgers, bedrijven en instellingen door hacking, DDoS-aanvallen, virussen en ransomware waardoor computersystemen buiten werking worden gesteld.

Ook stalking en bedreiging via internet nemen rap toe. Het zijn serieuze misdrijven die een verwoestende impact kunnen hebben op het leven van grote aantallen mensen en op onze economie. Hoe meer over ons bekend is, en hoe meer onze computersystemen met elkaar verbonden zijn, hoe kwetsbaarder we zijn voor deze vormen van criminaliteit.

De grote waarde van cybersecurity wordt ook benadrukt door de politie. Regelmatig roept die ons op om onze computer goed te beveiligen, onze wachtwoorden te veranderen en nooit ofte nimmer zomaar op een onbekende link te klikken. Gelijk heeft ze. We vormen vaak een veel te gemakkelijk doelwit zonder dat we ons dat bewust zijn. Tegelijkertijd hebben de politie en andere veiligheidsdiensten belang bij een zwakke databeveiliging. Via gaten in software, de zogenoemde *zero-days*, hacken ze namelijk zelf ook, in de hoop daarmee bewijs te verzamelen tegen mensen die ze van misdaden verdenken. Softwareleveranciers worden niet altijd gewaarschuwd na het ontdekken van deze kwetsbaarheden in hun product, waardoor de achterdeur blijft openstaan en criminelen kunnen binnenkomen. Het verzwakken van onze privacybescherming vormt een serieus risico voor de veiligheid van nietsvermoedende burgers en bedrijven, die de politie juist dient te beschermen.

Privacy is ook van belang voor een ander soort veiligheid: voor het recht om eerlijk behandeld te worden en niet te worden gediscrimineerd. Met de toenemende mogelijkheden om steeds meer data te verzamelen en te combineren, kunnen bedrijven en overheden conclusies over ons trek-