DATA-ANALYSE EN PRIVACY

Ronald Jeurissen

PRIVACY

In een samenleving die is gebaseerd op informatietechnologie (IT) stroomt informatie alsmaar sneller, breder en goedkoper in alle mogelijke richtingen. De analyse van deze groeiende stroom data blijkt voor allerlei organisaties zeer interessante toepassingen te bieden. Maar hoe zit het met de privacy van consumenten en burgers? Hebben consumenten hun privacy niet opgegeven, in ruil voor *gadgets* en comfort? Is de strijd tegen het terrorisme niet veel belangrijker dan privacy? Bedrijven begrijpen ondertussen dat het vertrouwen van klanten in de bescherming van hun privacy de nieuwe 'license to operate' wordt.

De analyse van big data wordt uitgevoerd door met gecompliceerde algoritmen te zoeken naar interessante verbanden in de enorme hoeveelheden data die mensen produceren met hun mobiele telefoons, hun e-mails, of in data die wetenschappers vinden in hun onderzoek. Enkele voorbeelden van de vele nuttige toepassingen van data-analyse:

- Door actuele gps-gegevens van haar gebruikers te analyseren, kan TomTom laten zien waar files staan en automobilisten alternatieve routes voorstellen.
- Door gegevens over haar eigen gebruikers te analyseren, kan LinkedIn bedrijven effectief adviseren over geschikte nieuwe medewerkers. Ook kan LinkedIn gemeenten adviseren over het talent-management in de regio.
- In Rusland is de app FindFace erg populair. Met behulp van deze app is het mogelijk om op straat een foto van iemand te maken en vervolgens de identiteit van deze persoon te achterhalen.
- Door e-mail en telefoonverkeer systematisch af te luisteren en te laten analyseren door computers, kunnen veiligheidsorganisaties als de AIVD terroristische aanslagen in een vroeg stadium op het spoor komen. Moderne chat-applicaties als WhatsApp en Signal bemoeilijken dit echter door hun berichten te versleutelen. Nationale veiligheidsdiensten willen dan ook zulke versleutelingen kunnen doorbreken, omwille van het algemeen belang.

Al deze toepassingen van data-analyse roepen vragen op over de privacy. Hoe ver mogen bedrijven en overheden gaan in het verzamelen, analyseren en exploiteren van de data van hun gebruikers? Deze vragen worden met de dag prangender omdat de hoeveelheden data die er over elke burger en elke consument beschikbaar komen, met de dag toenemen. Daarbij wordt in toenemende mate de aandacht gericht op zogeheten *ongestructureerde* data, dat wil zeggen gegevens die niet systematisch en volgens een van te voren bedachte vraag of structuur worden verzameld, maar die eerder spontaan worden gegenereerd, vaak als bijproduct van andere activiteiten. Zo blijkt de mobiele telefoon ook van moment tot moment te kunnen bijhouden waar iemand zich bevindt, hoewel het apparaat oorspronkelijk niet was bedoeld om zulke data te genereren. Berichten die mensen over het internet aan elkaar versturen, kunnen worden geanalyseerd op trefwoorden en zo op statistische wijze iets vertellen over welke sentimenten er leven in een populatie. In commerciële toepassingen wordt door fabrikanten tegenwoordig

steeds meer planmatig aangestuurd op het genereren van ongestructureerde data. Een voorbeeld is de Fitbit: een polsband die bio-informatie geeft over de gebruiker, zoals het slaappatroon, de hartslag, verbruikte calorieën en hoeveel stappen zijn gezet op een dag. Deze informatie is interessant voor de gezondheidsbewuste consument, maar bijvoorbeeld ook voor zijn verzekeraar, die wil weten hoe gezond verzekerden eigenlijk leven.

YAHOO MOEST IN SEPTEMBER 2016 TOEGEVEN DAT GEGEVENS VAN 500 MILJOEN GEBRUIKERS WAREN GESTOLEN

Zoals elke technologie kan ook de analyse van computerdata worden misbruikt en kunnen er fouten worden gemaakt die veel schade veroorzaken. Data van consumenten worden op grote schaal gehackt, waardoor wachtwoorden of creditcardgegevens in handen vallen van criminelen. Tijdens een hack in 2012 werden 117 miljoen inloggegevens van LinkedIn-gebruikers buitgemaakt. Op de site *haveibeenpwned.com* kunnen LinkedIn-gebruikers zien of hun eigen gegevens daarbij zijn. Inmiddels raadt LinkedIn haar leden aan om elke maand het wachtwoord te veranderen. Yahoo moest in september 2016 toegeven dat gegevens van 500 miljoen gebruikers waren gestolen, en dat dit reeds in 2014 was gebeurd. Veel bedrijven die worden gehackt hebben dit niet eens in de gaten, omdat de hackers geen sporen achterlaten. Het blijkt bovendien moeilijk te zijn voor consumenten om foutieve of ongewenste data over zichzelf van het internet te weren. 'Haatporno' is een nieuwe term voor pornografisch materiaal dat boze exen over hun gewezen partners op internet zetten. Voor degenen die het betreft is een gang naar de rechter nodig om zulke beelden van het internet verwijderd te krijgen. In Nederland is er nog geen wetgeving waarin dit goed is geregeld. Voor internetproviders is het voortdurend moeten verwijderen van content ondertussen een erg tijdrovende en kostbare bezigheid geworden.

Zonder vertrouwen in data-privacy komt er geen datagedreven economie, en dat vertrouwen is nog ver weg. De mogelijke veranderingen in de economie, in de samenleving en in het leven van individuele mensen zijn potentieel ook dermate ingrijpend dat een 'brede maatschappelijke discussie' over big data noodzakelijk is. Juist in het internettijdperk is het niet meer mogelijk om over het lot van mensen te beslissen zonder de mensen zelf te horen. Mensen zien de mogelijke baten van big data wel degelijk, maar ze zijn ook huiverig voor de risico's. De onzekerheid is dus groot, en deze zoekfase in de 'issues levenscyclus' van data-analyse gaat nog wel een paar jaar duren. In dit artikel wil ik aan de discussie bijdragen door enkele aspecten van data-privacy te verhelderen, waarbij wordt ingegaan op zowel juridische als ethische aspecten. Op welke wijze bedreigt data-analyse de privacy precies? Wat zijn de gevaren daarvan, en wat is er aan te doen? Om te beginnen moeten we echter onderzoeken wat privacy precies is, en waarom het belangrijk is.

HET BELANG VAN DATA-PRIVACY

Een korte en krachtige definitie van privacy is 'een toestand waarin men niet wordt geobserveerd of gestoord door andere mensen' (Oxford English Dictionary). Volgens artikel 12 van de VN Verklaring van de rechten van de mens (1948) hebben alle mensen hier recht op:

> 'Niemand zal onderworpen worden aan willekeurige inmenging in zijn persoonlijke aangelegenheden, in zijn gezin, zijn tehuis of zijn briefwisseling, noch aan enige aantasting van zijn eer of goede naam. Tegen een dergelijke inmenging of aantasting heeft een ieder recht op bescherming door de wet.'[1]

In de discussie over het belang van data-privacy worden vaak drie argumenten genoemd die zouden verklaren waarom data-privacy *niet* belangrijk is. Door deze argumenten kritisch te onderzoeken, komen we op het spoor van de diepere betekenis van data-privacy in het leven van burgers en consumenten.

Argument 1: Als je niets verkeerds doet, hoef je ook niet bang te zijn om gezien te worden

Privacy beschermt alleen de mensen die iets te verbergen hebben. Dit is een verleidelijk argument om data-privacy op te heffen. Het argument heeft ook zeker een kern van plausibiliteit: binnen de privésfeer doen mensen soms

inderdaad dingen die schadelijk zijn voor anderen, bijvoorbeeld ergens op een flatje een terroristische aanval voorbereiden. Het is niet goed dat mensen omwille van de privacy ongestoord ernstig de veiligheid en de openbare orde kunnen aantasten. Om die reden hebben politie en justitie vanouds ook allerlei bevoegdheden om de privésfeer van mensen binnen te dringen. Het ligt voor de hand om die bevoegdheden uit te breiden tot de sfeer van elektronische data en het mobiele telefoonverkeer. Maar het argument in algemene zin geeft een veel te ruime legitimatie voor het verzamelen van informatie over burgers en consumenten. De bewijslast lijkt te worden omgekeerd, door middel van de drogreden dat als je bang bent om gezien te worden, je blijkbaar iets verkeerds doet. Dat hoeft helemaal niet. Je kunt ook niet willen dat anderen je zien, gewoon omdat je vindt dat het hun zaken niet zijn, omdat je het niet prettig vindt om voortdurend geobserveerd en geanalyseerd te worden.

Wanneer mensen bloot staan aan de voortdurende analyse van hun data, over een breed spectrum van hun activiteiten, dan kan dat leiden tot ongemerkte vormen van sociale controle die de vrijheid van mensen aantast. Iemand die zichzelf ervaart als onderworpen aan publieke observatie, zal zich ook ervaren als onderworpen aan publieke beoordeling. Mensen zullen zich aanpassen aan wat zij denken dat de normen zijn die de dataverzamelaars over hen hanteren. Consumenten kunnen daar natuurlijk bewust voor kiezen, zoals de klanten van Fairzekering, die een kastje in hun auto laten inbouwen waarmee hun rijgedrag tot in details kan worden geanalyseerd. Wie veilig rijdt ontvangt van Fairzekering een korting op zijn autoverzekering.[2] Maar niet altijd wordt de keuze om geobserveerd en geanalyseerd te worden zo bewust gemaakt. Overmatige controle van mensen kan leiden tot een vlucht naar het midden in hun gedrag, omdat deviant gedrag wordt opgemerkt en misschien niet wordt gewaardeerd. Loopt je carrière gevaar als hoge ambtenaar wanneer je een datingsite bezoekt op internet? Of als je veel googelt op 'Bin Laden'? Mensen die zich voortdurend digitaal bekeken weten, nemen liever het zekere voor het onzekere. Ondertussen perken zij hun eigen vrijheid van handelen erg in.

WE MOETEN RUIM BINNEN DE GRENZEN BLIJVEN VAN WAT DE MAATSCHAPPIJ ACCEPTEERT EN VAN WAT TECHNISCH MOGELIJK IS

Men kan dit gedrag vergelijken met het befaamde Panopticum van Jeremy Bentham. Zijn ontwerp van een ronde gevangenis waarin één bewaker rondom alle gevangenen kon observeren, had als doel om op een efficiënte wijze het gedrag van criminelen positief te beïnvloeden. Alles wat ze in hun cel deden, kon door de bewaker worden gezien. De criminelen zouden daardoor de normen van de bewaker vanzelf overnemen, was de gedachte. Zulke panoptische gevangenissen zijn inderdaad gebouwd. Als blauwdruk voor een digitale samenleving, waar mensen vrijwillig voor zouden kiezen, is het echter geen aantrekkelijk en zelfs een ronduit beangstigend idee.

Argument 2: Privacy is overgewaardeerd: mensen zijn bereid het in te ruilen voor allerlei baten

Het gemak waarmee mensen tegenwoordig privacy opgeven op internet doet vermoeden dat zij helemaal niet in hun privacy geïnteresseerd zijn. Wie gebruik wil maken van elektronische netwerk- en communicatiediensten kan dat alleen door de algemene voorwaarden te accepteren, en daarin staan meestal heel ruime bepalingen over wat de dienstverlener mag doen met de data. Zo stelt het privacybeleid van WhatsApp:

> 'We verzamelen dienstgerelateerde, diagnostische en prestatiegegevens. Dit omvat informatie over uw activiteiten (zoals hoe u onze Diensten gebruikt, hoe u communiceert met anderen via onze Diensten, en dergelijke), logbestanden en diagnostische, crash-, website- en prestatieregistraties en -rapporten.'[3]

Andere digitale dienstverleners hebben vergelijkbare bepalingen. Hoe meer data van hun klanten zij mogen analyseren, hoe meer er met die data kan worden verdiend. Ondertussen gaat de consument schijnbaar zorgeloos akkoord met zulke contractuele bepalingen en lijkt privacy een geleidelijke dood te sterven.

De vraag is echter of het feitelijke consumentengedrag wel een goede indicator is van wat mensen willen. Dat ervoer bijvoorbeeld de bank ING toen het bedrijf in 2014 een proef aankondigde om klanten persoonlijke advertenties aan te bieden van andere bedrijven, op ba-

sis van hun betalingsgedrag. 'Als de proef succesvol is, wordt de dienst beschikbaar gemaakt voor alle 4,2 miljoen klanten die bankieren bij ING', aldus een woordvoerder. 'Klanten moeten expliciet aangeven dat ze mee willen doen. Het is een *opt-in* programma. Een tuincentrum wil bijvoorbeeld graag weten dat je elk jaar in maart 150 euro uitgeeft aan tuinspullen. Hij kan op het juiste moment een scherp aanbod doen', aldus directeur Particulieren Hans Hagenaars in het *Financieele Dagblad*. Adverteerders stonden volgens hem in de rij om mee te doen. Natuurlijk begreep ING dat het plan raakte aan de privacy van klanten. 'We moeten dan ook ruim binnen de grenzen blijven van wat de maatschappij accepteert. Ook al is er technisch meer mogelijk', zei Hagenaars. Direct na deze aankondigingen stak er een storm van protest op. *No way* dat de bank mijn gegevens hiervoor ooit mag gebruiken, vonden vele ING-klanten. Dat het om een *opt-in* programma ging, maakte blijkbaar niet veel uit. Dat klanten veel meer van hun privacy weggeven aan Google of Facebook is blijkbaar ook geen punt van overweging. Van de eigen bank verwachten consumenten blijkbaar toch een heel ander privacy-beleid dan van een website waar je plaatjes van de baby en de poes deelt met anderen.

Als burgers hechten mensen vaak wél aan hun privacy en zijn zij kritisch over wat bedrijven met hun data doen. Volgens een survey uit 2014 van het PEW Research Center voelt 68 procent van de geïnterviewde Amerikaanse volwassenen zich niet veilig om privé-informatie te versturen via chat- of instant-messagediensten en voelt 57 procent van de ondervraagden zich niet veilig om zulke informatie te versturen via e-mail.[4] Consumenten die op het punt staan om een ondoorzichtig en omvangrijk document met algemene voorwaarden te tekenen van een of andere digitale dienstverlener, voelen zich geconfronteerd met een zogeheten 'collective goods'-probleem. Als burgers vinden we wel dat privacy een belangrijk collectief goed is, maar deze ene kleine beslissing van mij als consument tast dat collectieve goed nauwelijks aan. Omdat alle consumenten zo redeneren, is de som van alle kleine beslissingen toch dat het collectieve goed wordt opgeofferd. De klassieke uitweg uit het *collective goods*-probleem is dat het collectieve goed wordt beschermd door een afspraak tussen burgers onderling, of door wetgeving. Als burgers moeten we dus gezamenlijk werken aan regelingen waarmee we onze onvoorzichtigheid en kortzichtigheid als individuele consument in bedwang houden.

Argument 3: Sommige maatschappelijke belangen zijn groter dan privacy

Het argument dat hier altijd weer van stal wordt gehaald is dat van de nationale veiligheid. Het Amerikaanse Congres nam op 26 oktober 2001, vlak na de aanval op de Twin Towers, een wet aan genaamd de *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism* Act. De stoere afkorting van deze wet is 'USA PATRIOT' en dat brengt ons onmiddellijk in de oorlogszuchtige sfeer die president Bush indertijd verspreidde met zijn 'wie niet voor ons is, is tegen ons'. We zijn in oorlog met de terroristen en bij de mobilisatie voor de oorlog hoort dat er nu even geen tijd is voor privacy. De USA PATRIOT Act regelt de wijze waarop Amerikaanse veiligheidsdiensten informatie vergaren over iedereen en optreden in geval van mogelijk terrorisme. De wet geeft onder meer toestemming voor het afluisteren van de regeringen van andere landen, wat leidde tot onder andere het afluisteren van de telefoon van Bondskanselier Angela Merkel.

Ook hier is weer sprake van een belangrijke redeneerfout, namelijk dat veiligheid een zaak is van groot nationaal belang, en privacy slechts een klein individueel belang dient. De optelsom van ieders individuele privacy is ook een groot nationaal belang. Privacy is namelijk essentieel voor het onderhouden van de democratie in een land. Privacy beschermt de ruimte van autonomie die mensen nodig hebben om weerbare en onafhankelijke democratische burgers te zijn. Het is geen toeval dat in alle dystopische toekomstromans de privacy het eerste is wat de machthebbers elimineren: 'Big Brother is watching you'. Het is ook geen toeval dat uitgerekend in China de privacy van de burgers op internet en social media het hardst wordt uitgehold. Dat ervoer Google, toen het door de Chinese overheid werd gedwongen om gegevens over dissidente burgers te overhandigen, terwijl er

PRIVACY IS ESSENTIEEL VOOR HET ONDERHOUDEN VAN DE DEMOCRATIE IN EEN LAND

ook pogingen werden ondernomen om zulke gegevens te hacken. Op dit moment wordt in China een digitale database van alle burgers voorbereid die in 2020 live moet gaan. Daarin wordt het 'burgerschap' van elke Chinees vastgelegd in een rangschikking, die wordt bepaald door zaken als fiscaal gedrag, kredietwaardigheid en gedrag in het verkeer. Chinezen mogen er nu al speels mee kennis maken, via Sesame Credit, de financiële tak van de koopsite Alibaba, dat 400 miljoen gebruikers heeft.[5] De Chinese regering begrijpt heel goed dat zij haar burgers ertoe moet verleiden om geen waarde te hechten aan privacy, om daarmee het streven naar meer democratie te frustreren. Anderzijds moet ook worden erkend dat in de Chinese collectieve cultuur, waarin familie en staat belangrijke waarden vertegenwoordigen, het individu met zijn rechten en belangen een lagere plaats op de waardenladder inneemt dan in westerse samenlevingen.

REDENEN OM DE PRIVACY VAN CONSUMENTEN BETER TE BESCHERMEN

Het is belangrijk om de privacy van consumenten en burgers te beschermen in de wereld van de data-analyse, en er zijn drie redenen om dat te doen: omdat het moet, omdat het loont en omdat het hoort. De eerste reden verwijst naar de wet, de tweede naar de markt en de derde naar de ethiek. De wetgever heeft, vooral op Europees niveau, zeer stringente wetgeving ontwikkeld om de privacy van zijn burgers te beschermen. Bedrijven zien bovendien ook zelf in dat 'big data' een kip met gouden eieren is, die men niet moet slachten. Het is dus ook uit welbegrepen eigenbelang dat bedrijven een reden hebben om zorgvuldig om te gaan met de privacy van hun klanten. Tenslotte hebben de meeste mensen ook een moreel besef en een morele verantwoordelijkheid. In een samenleving van mondige en verantwoordelijke burgers is ook de ethiek een factor die kan bijdragen aan de oplossing van maatschappelijke vraagstukken.

OMDAT HET MOET …

De Europese privacy-wetgeving hoort tot de meest stringente ter wereld. De Nederlandse Wet Bescherming Persoonsgegevens (Wbp), die op 1 januari 2016 van kracht is geworden, bepaalt wat een persoonsgegeven is en stelt regels voor de verwerking daarvan. Een persoonsgegeven is 'elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon'. Verwerken van persoonsgegevens betreft: 'elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens.' (Art. 1 Wbp).

Artikel 8 van de Wbp onderwerpt het verwerken van persoonsgegevens aan een serie zeer stringente beperkingen. 'Persoonsgegevens mogen slechts worden verwerkt indien:

a. de betrokkene voor de verwerking zijn ondubbelzinnige toestemming heeft verleend;
b. de gegevensverwerking noodzakelijk is voor de uitvoering van een overeenkomst waarbij de betrokkene partij is, of voor het nemen van precontractuele maatregelen naar aanleiding van een verzoek van de betrokkene en die noodzakelijk zijn voor het sluiten van een overeenkomst;
c. de gegevensverwerking noodzakelijk is om een wettelijke verplichting na te komen waaraan de verantwoordelijke onderworpen is;
d. de gegevensverwerking noodzakelijk is ter vrijwaring van een vitaal belang van de betrokkene;
e. de gegevensverwerking noodzakelijk is voor de goede vervulling van een publiekrechtelijke taak door het desbetreffende bestuursorgaan dan wel het bestuursorgaan waaraan de gegevens worden verstrekt, of
f. de gegevensverwerking noodzakelijk is voor de behartiging van het gerechtvaardigde belang van de verantwoordelijke of van een derde aan wie de gegevens worden verstrekt, tenzij het belang of de fundamentele rechten en vrijheden van de betrokkene, in het bijzonder het recht op bescherming van de persoonlijke levenssfeer, prevaleert.'

Bovendien hebben burgers een groot aantal rechten ten aanzien van over hen verwerkte data, zoals het recht op informatie, recht op inzage, op verbetering, aanvulling, ver-

wijdering of afscherming, het recht op verzet en ten slotte het 'recht om te worden vergeten'. Dat laatste gaat terug op een uitspraak van het Europese Hof van Justitie in een zaak die een Spanjaard had aangespannen tegen Google, betreffende een aantal nieuwsberichten die via Google op de website van een krant te vinden waren over zijn zakelijke schulden in het verleden. Hij wilde die informatie van het web af hebben. Het Hof oordeelde dat de berichten op de site van de krant mochten blijven staan, maar dat Google de links naar deze berichten diende te verwijderen.

De discussie over privacywetgeving op het internet is momenteel in volle gang. Het Rathenau-instituut en de Wetenschappelijke Raad voor het Regeringsbeleid (WRR) hebben er uitvoerige studies aan gewijd. Het Rathenau-Instituut onderzoekt de vraag 'Wat nu, als je straks meer moet betalen voor je verzekering, omdat de data van je fitnessarmbandje, facebookprofiel en onlinekoopgedrag aantonen dat je een ongezonde, risicovolle levensstijl hebt?' (Timmer e.a., 2015). De WRR beveelt aan dat de aandacht wordt verlegd van het reguleren van het verzamelen van data – het zwaartepunt in de huidige juridische kaders – naar de regulering van en het toezicht op de fases van de analyse en het gebruik van persoonsgegevens (WRR, 2016).

BEDRIJVEN BESEFFEN DAT 'BIG DATA' EEN KIP MET GOUDEN EIEREN IS, DIE ZE NIET MOETEN SLACHTEN

Een belangrijk onderdeel van het privacy-vraagstuk voor de komende decennia wordt het vinden van een balans tussen de belangen van consumenten en de belangen van de organisaties die data-analyses willen uitvoeren, inclusief de overheid die claimt omwille van de veiligheid en criminaliteitsbestrijding in principe alle data te moeten kunnen doorzoeken,. Momenteel is het zo dat de strenge privacy-wetgeving een forse rem zet op technologische ontwikkelingen, wanneer onderzoekers voor elke nieuwe data-analyse die zij bedenken eerst langs alle betrokkenen moeten om toestemming te vragen. Onderzoek naar nieuwe medicijnen kan hierdoor vertraging oplopen.

OMDAT HET LOONT …

Bedrijven die gebruik maken van data-analyse doen er verstandig aan om te blijven opereren binnen de grenzen van de wet en wat maatschappelijk als betamelijk geldt. De 'license to operate' is in het geding. De verwachting is dat bedrijven omwille van hun reputatie een zekere mate van zelfbeheersing aan de dag zullen leggen en niet te veel inbreuk zullen plegen op de privacy van hun klanten. Is dit een gerechtvaardigde verwachting, of is dit ijdele hoop? Om dat te beoordelen, moeten we bekijken onder welke voorwaarden het reputatiemechanisme werkt. Het werkt namelijk niet wanneer er geen herhaalde transacties zijn, en het werkt ook niet wanneer de tijdsspanne tussen oorzaak en gevolg te lang is. In het ene geval hebben we te maken met een 'market for lemons', naar het gelijknamige artikel van de econoom Akerlof, die dit mechanisme voor het eerst wetenschappelijk beschreef (Akerlof, 1970). Wanneer een verkoper verwacht dat hij zijn koper na de transactie nooit meer zal zien, is hij niet geneigd om belang te hechten aan zijn reputatie en zal hij geneigd zijn om te profiteren ten koste van de koper. Mede door het internet zijn zulke eenmalige transacties echter toch met elkaar in verband te brengen, namelijk door feedback van verschillende gebruikers te verzamelen, zoals op boekingssites veel gebeurt. Van een ander geval waarin het reputatiemechanisme niet werkt, is sprake als de effecten worden verdonkermaand door de tijd. Zo was de tabaksindustrie zich lange tijd zeer bewust van de schadelijke gezondheidseffecten van tabak, maar omdat de incubatietijd decennia kan duren, ging er geen reputatie-prikkel van uit. Voor overtredingen van de privacy door data-analisten gelden beide negatieve moderatoren van het reputatiemechanisme echter niet. De eerder beschreven ING-kwestie laat zien dat bedrijven er verstandig aan doen om transparant te zijn over wat zij met data van klanten doen.

OMDAT HET HOORT …

De vraag hoe het hoort is de vraag naar de ethiek. In de eerste helft van dit artikel zijn al enkele ethische overwegingen gemaakt ten aanzien van het belang van data-privacy. De vraag die nog open staat, is of de ethiek, de eigen

morele oordeelsvorming en de eigen verantwoordelijkheid van mensen en organisaties, een rol kan spelen in het bevorderen van data-privacy.

Twee manieren waarop bedrijven vrijwillig kunnen omgaan met hun maatschappelijke verantwoordelijkheid zijn de gedragscode en conventanten. Dit kan worden geïllustreerd aan de hand van de privacy-verklaring van Iddink, een bedrijf uit Ede dat zich richt op de educatieve dienstverlening. In deze verklaring stelt Iddink dat het de privacy van alle gebruikers respecteert en alle persoonsgegevens verwerkt op een behoorlijke, vertrouwelijke en zorgvuldige wijze zoals is voorgeschreven door de Wbp.[6] Iddink is ook aangesloten bij het 'Convenant Digitale Onderwijsmiddelen en Privacy' dat de Wbp vertaalt naar de onderwijspraktijk. Bij dit convenant zijn tientallen partijen uit de educatieve wereld aangesloten. Dit convenant bevat afspraken over het omgaan met persoonsgegevens bij het gebruik van digitale leermiddelen en toetsen. 'Dankzij het convenant weten scholen en aanbieders wat ze over en weer van elkaar mogen verwachten, zijn de afspraken werkbaar in de praktijk en heeft iedereen dezelfde gemeenschappelijke uitleg bij deze afspraken.'[7] De doelstelling van het convenant is gericht op het bevorderen van het vertrouwen in de digitale ontwikkelingen binnen het onderwijs.

Ik wil eindigen met een gedachte over de beroepsethiek van IT-professionals. Deze gedachte is geopperd door de Amerikaanse ethicus Deborah Johnson, in haar boek *Computer Ethics*. Aan het slot van dit zeer lezenswaardige boek stelt zij de vraag of IT-specialisten 'guns for hire' zijn, of *professionals*. Zij eindigt met de volgende even simpele als betekenisvolle conclusie hierover: 'Given the efficacy of computer experts and the dependence of the public on the work of computer experts, it seems critical that computer experts take responsibility for safe and reliable computing' (Johnson, 2009, p. 192). Geen 'guns for hire' dus.

In de IT-wereld is momenteel al een aantal gedragscodes voor IT-professionals in omloop. Een voorbeeld is de code van de werkgroep Ethiek (Ethics Workgroup) van de Finse brancheorganisatie voor informatieverwerking (Finnish Information Processing Association), welke stelt dat 'IT-professionals hun macht niet mogen misbruiken. Zij moeten hun verantwoordelijkheid nemen, die kan worden gemeten in termen van handelingen en verrichtingen. Kennis is macht, en kennis gebruiken vraagt om wijsheid, net zoals ieder gebruik van macht'.[8] Op dit moment is vooral de morele verantwoordelijkheid groot van de mensen die de algoritmen bedenken op basis waarvan data-analyses worden uitgevoerd. In deze algoritmen worden immers morele beslissingen versleuteld en morele uitgangspunten omgezet in nullen en enen. Het is van groot belang dat hieraan aandacht wordt besteed in de opleidingen voor data-analisten aan Hogescholen en Universiteiten.

Noten

1. De term 'briefwisseling' in dit artikel is wel aan uitbreiding toe, want de schriftelijke communicatie gaat tegenwoordig grotendeels via elektronische berichten.
2. Zie: www.fairzekering.nl
3. https://www.whatsapp.com/legal/#privacy-policy-information-we-collect
4. http://www.pewinternet.org/2014/11/12/public-privacy-perceptions/
5. http://www.bbc.com/news/world-asia-china-34592186
6. https://www.iddink.nl/pdf/privacyverklaring.pdf
7. http://www.privacyconvenant.nl/
8. http://www.tivia.fi/sites/d7.tivia-new.fi/files/tivia/Julkaisut/Etiikan_ohjeet/FIPA%20ethics%20code%20-%20unofficial%20translation%20(2).pdf (eigen vertaling)

Literatuur

Akerlof, G. (1970). The Market for 'Lemons': Quality Uncertainty and the Market Mechanism. *The Quarterly Journal of Economics*, 84 (3), pp. 488-500.

Johnson, D. (2009). *Computer Ethics*. Upper Saddle River: Pearson, 4e ed.

Timmer, J., I. Elias, L. Kool & R. van Est (2015). *Berekende risico's: Verzekeren in de datagedreven samenleving*. Den Haag: Rathenau Instituut.

Wetenschappelijke Raad voor het Regeringsbeleid (2016). *Big Data in een vrije en veilige samenleving*. Amsterdam: Amsterdam University Press, WRR Rapporten, nr. 95.

Over de auteur

Prof. dr. R.J.M. Jeurissen is Hoogleraar Bedrijfsethiek aan Nyenrode Business Universiteit.