Bedwelmende zelfontplooiing[1]

Bart Jacobs

Informatie- en communicatietechnologie (ICT) beïnvloedt de maatschappij ingrijpend. Deze uitspraak is inmiddels een cliché: productieprocessen zijn nu computergestuurd, nieuwe vormen van dienstverlening (op afstand) zijn ontstaan, en burgers hebben meer mogelijkheden dan ooit om te communiceren, informatie tot zich te nemen en informatie te verspreiden. De overheid en private partijen hebben vergaande mogelijkheden om het gedrag van burgers in detail te volgen en hun 'diensten' op dit gedrag aan te passen. De veranderingen aan de oppervlakte zijn duidelijk zichtbaar, bijvoorbeeld in de alomtegenwoordigheid van *smartphones* met ongekende mogelijkheden. Maar wat zijn de veranderingen die deze nieuwe technologieën op een dieperliggend niveau met zich mee brengen? Hoe zijn bijvoorbeeld de (machts)verhoudingen in de samenleving veranderd?
Dit hoofdstuk zal puntsgewijs een aantal van zulke veranderingen belichten, uitgaande van specifieke aspecten van de techniek. De nadruk zal daarbij liggen op de informatiestromen. Met het idee 'informatie is macht' als leidraad zal in het bijzonder gekeken worden naar wie toegang heeft tot informatiestromen (en wie daarover besluit). Vanzelfsprekend komen hierbij ethische en politieke vragen naar voren. Die vragen zal ik hier en daar expliciteren, maar niet beantwoorden.
De veranderingen en trends die hieronder genoemd worden zijn afkomstig uit de vakliteratuur, uit gesprekken met collega's en uit eigen ervaringen en overpeinzingen. Er is geen enkele pretentie dat de lijst volledig is en er is, gegeven de beperkte omvang van deze tekst, ook geen sprake van uitputtende behandeling. Hopelijk helpt deze uiteenzetting desondanks om patronen te herkennen in de ontwikkelingen van de afgelopen decennia.

Informatie en drager

Een boek biedt de lezer informatie, in de vorm van de tekst die erin gedrukt staat. Tegelijkertijd vormt een boek de drager van die informatie, als samengebonden lijst van bladzijden. Traditioneel zijn we

1 Verschenen in: Tobias Kwakkelstein, Aart van Dam en Ardaan van Ravenzwaaij (red), Van verzorgingsstaat naar waarborgstaat. Nieuwe kansen voor overheid en samenleving, Boom, Den Haag 2012, p.85-97.

gewend aan een dergelijke eenheid van informatie en drager. Langspeelplaten, dossiermappen, schilderijen enzovoort zijn fysieke dragers die onafscheidelijk van hun inhoud voorkomen. Door digitalisering is die eenheid van drager en informatie verloren gegaan: eenmaal gedigitaliseerde werken zijn oneindig vaak kopieerbaar, zonder verlies van kwaliteit, en kunnen makkelijk en zeer snel van de ene op de andere drager worden overgezet, bijvoorbeeld van de harde schijf op een webserver aan de andere kant van de wereld, naar de eigen USB-stick. Dit is een fundamentele verandering met vergaande gevolgen. Bijvoorbeeld is controle over informatie (zoals censuur) veel makkelijker wanneer je die controle kunt uitoefenen over de productie of verspreiding van de drager. De muziek-, film- en boekensector worstelt nog steeds met deze verandering en toont moeite (of onwil) om tot een ander commercieel paradigma te komen. De verloren eenheid van informatie en drager is ook een uitdaging voor ons juridische kader: wat is de waarde van informatie, als immaterieel goed? Wat betekent het stelen van informatie precies (PIN-code, of punten/trofeeën in een game)? Op het gebied van auteursrecht neemt de spanning toe met privacyrecht: controle verplaatst zich van de dragers naar de individuele gebruiker. Op het gebied van handel en recht zien we de laatste decennia een overgang van goederen naar digitale diensten.
WikiLeaks toont enerzijds hoe lastig het is om geheime digitale informatie adequaat af te schermen en anderzijds dat pikante, eenmaal openbaar geworden informatie niet meer onder controle te krijgen is. In de gezondheidszorg hebben zorgverleners een dossierplicht met bijbehorende plicht tot geheimhouding. Van oudsher denkt men aan een zware afsluitbare dossierkast in het kantoor van de arts. Daar is echter allang geen sprake meer van. De politieke en maatschappelijke onrust rond het Elektronisch Patiënten Dossier (EPD) is grotendeels terug te voeren op het ongemak dat mensen hebben bij de teloorgang van dergelijke fysieke controle. Het EPD probeerde tegelijkertijd een wettelijk kader (inclusief vereisten) en een infrastructuur te geven voor de omgang met digitale medische informatie.

Drager en kanaal

De internetpioniers van het eerste uur vonden dat informatie vrij moest zijn. Zij zagen de zojuist beschreven scheiding van informatie en drager als bevrijding en *empowerment,* die het individu meer ontplooiingsmogelijkheden en macht gaf, onafhankelijk van de ‘grote partijen’ die invloed uitoefenen via controle over informatiedragers. Tegelijkertijd meenden ze dat autoriteiten gedwongen zouden worden tot een grotere mate van transparantie (en eerlijkheid). Die gedachte is nog springlevend bij de aanhangers van WikiLeaks. Nu echter moeten we constateren dat het uiteindelijk vooral burgers zijn die tot transparantie gedwongen zijn, en niet zozeer de autoriteiten. Het gaat er nu niet meer om wie de

dragers van informatie beheerst, maar wie de informatiekanalen controleert.
De telefoon, zeker in mobiele vorm, is een mooi voorbeeld van een techniek die leidt tot empowerment, bevrijding en ontplooiing van het individu (en zelfs individualisering tegengaat). Autoriteiten realiseerden zich echter snel dat de telefoon ook ontplooiingsmogelijkheden biedt aan individuen met minder prettige bedoelingen en hebben rap bevoegdheden geïntroduceerd om te kunnen zien wie met wie communiceert en om gesprekken af te kunnen luisteren. Vergelijkbare afgedwongen toegang tot het communicatiekanaal bestaat op internet, gericht op afluisteren of zelfs filtering (blokkering) van bepaalde informatie. De *great Chinese firewall* is een berucht voorbeeld, dat door tientallen andere landen enthousiast nagevolgd wordt.
Tegenmacht richt zich vooral op het doorbreken van dergelijke controle over het informatiekanaal, voornamelijk via *end-to-end* versleuteling of via een combinatie van maskering van de route en versleuteling. Software daarvoor, zoals PGP en Tor, is gratis beschikbaar. Westerse overheden nemen een ambigue houding aan: enerzijds stimuleren ze het gebruik van dergelijke technieken door dissidenten in verre landen en anderzijds proberen ze het gebruik ervan door eigen burgers zo veel mogelijk tegen te werken, bijvoorbeeld via nieuwe inbraakbevoegdheden op computers van verdachten (om wachtwoorden te kunnen achterhalen en versleuteling te kunnen doorbreken) of via nieuwe bevoegdheden om internetverkeer grootschalig te monitoren.

Broadcast en point-to-point

Radio- en televisiesignalen worden van oudsher door krachtige antennes via de ether verspreid. De luisteraar of kijker pikt de signalen via een eigen antenne uit de lucht, en selecteert lokaal de gewenste zender. Deze lokale selectie uit een breed spectrum is het kenmerk van wat heet een *broadcast*-model van verspreiding: iedereen krijgt alle informatie en maakt uit dit brede aanbod een eigen keuze, zonder dat de verzender van de informatie deze keuze kan observeren. De nieuwsvoorziening via de krant werkt ook met dit broadcast-model. Ik ontvang dagelijks de gehele krant, en lees daarin alleen wat mij interesseert. De verzenders van de informatie, in Hilversum of op de redactie van de krant, weten niet welke programma's ik bekijk of welke artikelen ik lees.
Dit broadcast-model wordt steeds meer vervangen door een *point-to-point*-model. Als ik mijn nieuws lees via de website nu.nl klik ik alleen een item aan dat me boeit. Vervolgens stuurt mijn computer dit verzoek door naar de webserver van nu.nl. Die stuurt de opgevraagde webpagina, speciaal voor mij, naar het IP-adres van mijn computer, zodat ik de pagina kan bekijken. In een point-to-point-model stuurt de verzender mij dus niet alle informatie, maar alleen die waar ik naar vraag. Dit lijkt veel

efficiënter dan broadcast; inderdaad, de sportbijlage van de krant gooi ik altijd ongelezen weg. Iedereen tevreden?

Deze verandering van broadcast naar point-to-point heeft echter vergaande consequenties. De verzender van de informatie kan plotseling in detail bijhouden wie, wanneer en hoe lang waar naar kijkt (en hoe vervolgens verder geklikt wordt). Technisch gezien gebeurt dit via *cookies*, via het IP-adres, of via andere unieke eigenschappen van mijn computer (zoals een *browser fingerprint*). Deze gedragsinformatie is goud waard en vormt de basis voor uitgebreide profielen die van gebruikers opgebouwd worden en als basis dienen voor gerichte aanbiedingen of uitsluitingen. De sector zegt: we zijn u hiermee van dienst, en sturen u alleen reclame waarin u echt geïnteresseerd bent. Dit is natuurlijk onzin. De adverteerders sturen de informatie waarvan zíj willen dat ik die zie, niet van wat ík zelf wil (zie ook Jacobs, 2011). Daarnaast bepalen zij ook, of ik uitgesloten wordt van bepaalde aanbiedingen (zoals een gunstige hypotheek). Bewustwording van deze op de persoon gerichte beïnvloedingsmechanismen geeft mensen vaak een ongemakkelijk gevoel. Een fundamentele vraag is of ik het recht heb van deze weinig transparante manipulatie verschoond te blijven, en bijvoorbeeld ook onbespied nieuws tot mij kan nemen in een point-to-point-model. Dit raakt aan basale vrijheden in een democratie. Moet de overheid niet alleen de pluriformiteit in de media bevorderen maar ook de vrije, onbespiede toegang daartoe? Gevoeligheid voor deze materie is niet wijd verbreid.

Zenden en ontvangen

In de huidige vorm zegt artikel 7 van de Nederlandse Grondwet: ‘Niemand heeft voorafgaand verlof nodig om door de drukpers gedachten of gevoelens te openbaren, behoudens ieders verantwoordelijkheid volgens de wet.’ De gedachte achter dit artikel moge helder zijn, maar de techniekafhankelijke formulering is duidelijk achterhaald. De afgelopen jaren heeft een Staatscommissie zich gebogen over de modernisering van de Grondwet, in deze en andere artikelen. Juist door de eerdergenoemde onafhankelijkheid van informatie en drager zijn de individuele mogelijkheden om informatie te verzenden sterk toegenomen, bijvoorbeeld via blogs en tweets. Van beperkingen op openbaring is in de praktijk niet of nauwelijks sprake.

Het geciteerde zevende artikel van de Grondwet richt zich op het verzenden van informatie. Dit is min of meer vanzelfsprekend geworden. Minder vanzelfsprekend echter wordt het ontvangen van informatie. Commerciële partijen (maar ook overheden) hebben er belang bij dat ik bepaalde informatie wel zie en andere niet, waardoor ik mogelijk eerder geneigd ben tot een aankoop (of tot politieke

inertie). Door vergaande profilering zijn informatiediensten persoonlijk geworden. Eenzelfde zoekopdracht bij Google geeft bij verschillende mensen verschillende uitkomsten: de zoekterm 'Egypte' leidt bij mij mogelijk tot informatie over strandvakanties en bij u over activisten. Google meent te weten dat de een meer geïnteresseerd is in dit, en de ander meer in dat. Google (en vergelijkbare diensten) zijn niet objectief, en zijn er zelfs open over dat ze ons zo betuttelen. Ze presenteren het als een 'dienst'. Ze zijn er echter niet open over hoe ze zoekresultaten per gebruiker selecteren en door wiens belangen de individuele manipulatie gestuurd wordt (zoals bijvoorbeeld touroperators naar Egypte). In Pariser (2010) wordt daarom gesproken van een *information bubble* waarin ieder van ons in een eigen wereld leeft en waarin partijen die de informatiestromen beheersen bepalen wat wij individueel wel of niet te zien krijgen. Daarbij wordt nadrukkelijk de zorg uitgesproken dat het idee van een gedeelde gemeenschappelijke ruimte en (historische) ervaring verloren gaat, leidend tot voortgaande sociale fragmentatie. Morozov (2011) schrijft: 'What if the liberating potential of the Internet also contains the seeds of depoliticization and thus dedemocratization?'

In de krantenwereld is op een gegeven moment een scheiding ontstaan tussen bedrijf en inhoud: de redactie wordt gedreven door journalistieke professionaliteit en de onafhankelijkheid daarvan wordt door de kranteneigenaren gegarandeerd. Daarbij hebben verschillende kranten wel degelijk verschillende politieke kleuren, maar die voorkeur is meestal redelijk transparant, bijvoorbeeld uit redactionele commentaren en opgebouwde reputatie. Bij zoekmachines is nog lang geen sprake van een dergelijke scheiding tussen financiële en inhoudelijke belangen. Ook is nog onvoldoende uitgekristalliseerd wat de politieke kleur is van bijvoorbeeld Google of Yahoo.

De eerdergenoemde Staatscommissie heeft zich bewust getoond van deze ontwikkelingen door als nieuwe formulering van het eerste en tweede lid van artikel 7 voor te stellen: '1. Niemand heeft voorafgaand verlof nodig om gedachten en meningen te openbaren, behoudens ieders verantwoordelijkheid volgens de wet. 2. Het ontvangen van informatie is vrij, behoudens beperkingen bij de wet gesteld.' Dit is mooi, maar heeft vooralsnog de status van een voorstel.

Vergeten en onthouden

Mensen moeten moeite doen om dingen te onthouden; vergeten gaat helaas vanzelf. In de wereld van ICT is het omgekeerde het geval: eenmaal opgeslagen informatie wordt eindeloos onthouden, en gaat niet verloren, tenzij een expliciete *delete* opdracht gegeven wordt (Mayer-Schönberger, 2009). In de hersenen opgeslagen informatie moet ververst worden door regelmatig hergebruik en verwerking in een

nieuwe context. Digitaal opgeslagen informatie blijft in principe onveranderd. Door de technische ontwikkelingen is het wel nodig de informatie van tijd tot tijd op een nieuwe drager te plaatsen, bijvoorbeeld van floppy naar USB-stick of harde schijf. Inhoudelijke verversing en herbewerking is echter niet nodig voor het voortbestaan. Een grotere bedreiging voor de toegankelijkheid is onvindbaarheid, door overdaad aan informatie maar ook door slechte archivering. Slimme zoektechnieken helpen bij het beheersen van grote hoeveelheden informatie, maar zijn machteloos bij slordig beheer.

Alles onthouden lijkt ideaal. Dat geldt echter niet voor degene van wie een beschamende foto op internet verschenen is, of voor iemand die zijn straf uitgezeten heeft en zijn leven weer op de rails wil zetten. Een eigen, nieuwe invulling aan je leven kunnen geven, wordt gezien als een belangrijk onderdeel van persoonlijke autonomie en privacy, zie ook de sterk op zelfontplooiing gerichte formulering in Agre en Rotenberg (1997): ‘the right to privacy is the freedom from unreasonable constraints on the construction of one’s identity’. Een mogelijk recht op vergeten is onderdeel geworden van het moderne debat (Buruma, 2011). In Mayer-Schönberger (2009) wordt voorgesteld iedere keer bij het opslaan van een document aan te geven wanneer het document (automatisch) weer verwijderd moet worden. Deze aanpak is erg simplistisch. Maar een meer verfijnde technische oplossing die beter aansluit bij onze biologische vergeetachtigheid is sociaal wel degelijk gewenst.

Identiteiten en attributen

Bij het kopen van een fles whisky moet je laten zien dat je boven de 18 bent. In de praktijk waai je bij de slijter even met je paspoort of identiteitskaart. Stel echter dat de winkelier je document even vast wil houden, om een kopie te maken of om de chip die erin zit uit te lezen. Daarmee verkrijgt hij veel meer informatie dan voor de aankoop nodig is: volledige naam, geboortedatum, BSN, digitale foto, enzovoort. Het is duidelijk dat dit een onacceptabele overkill is, die een risico vormt voor het individu: identiteitsfraude (iemand anders sluit met de gegevens bijvoorbeeld een lening af op jouw naam) of profilering (precies bijhouden wie wanneer hoeveel drank koopt). Zulke informatie kan gebruikt worden voor gerichte reclame (om alcoholisten nog meer te laten drinken), om door te verkopen aan derden, en mogelijk zelfs om iemand te chanteren. Daarnaast bestaat altijd het risico dat door (technische) slordigheden dergelijke informatie publiek bekend wordt. De vele lekken van de laatste jaren tonen dat de kans daarop niet heel klein is.

Het onderliggende issue is dat voor de whisky-transactie enkel het attribuut ‘boven de 18’ nodig is, en niet de precieze identiteit van de koper. Op eenzelfde wijze is voor het reizen met het openbaar vervoer

enkel een geldig kaartje nodig, en niet je identiteit (zoals vastgelegd via het nummer van de OV-chipkaart). Opvallend is dat bij digitalisering van velerlei diensten attributen vervangen worden door identiteiten. Dit heeft grote gevolgen voor de privacy en voor de risico's (met name op identiteitsfraude) die individuen lopen. Er zijn twee belangrijke redenen voor deze transitie van attributen naar identiteiten. Allereerst hebben de dienstenleveraars (de Google's, Translink Systems, enz.) er commercieel belang bij hun klanten tot in detail te kennen, namelijk om die informatie te gebruiken voor het verbeteren van hun diensten en voor het versturen gerichte reclame en mogelijk zelfs voor de verkoop van de resulterende profielen. Ten tweede is het vaak de meest voor de handliggende weg om ICT-systemen op identiteiten te baseren in plaats van op attributen. Pas sinds een jaar of tien zijn er betrouwbare cryptografische technieken voorhanden (zoals U-Prove en Idemix) voor het gebruik van attributen. Daarmee kan adequaat vorm worden gegeven aan de plicht tot dataminimalisatie en kan serieus werk worden gemaakt van de moderne eis tot *privacy-by-design*.

Centraal en decentraal

De aloude agenda in de binnenzak is bij veel mensen vervangen door een online agenda bij Google. Waar persoonlijke gegevens van oudsher decentraal, bij de betrokkenen zelf, beheerd werden, worden die gegevens nu centraal bijgehouden ‘in de *cloud*’. Ook deze transitie doet zich op meer gebieden voor: een traditionele elektriciteitsmeter is een lomp apparaat in de meterkast, waarin een schijf langzaam ronddraait en een tellertje het cumulatieve gebruik bijhoudt. Een moderne ‘slimme’ meter is een computertje dat ieder kwartier het actuele verbruik doorgeeft aan de centrale computer van de elektriciteitsleverancier. In de tijd voor de sociale media wisten alleen mensen in je directe omgeving je nieuwtjes, ervaringen en voorkeuren. Nu staan al die details op centrale servers bij Facebook en Hyves. Die gegevens worden door deze informatiegiganten voortdurend geanalyseerd en op allerlei manieren gebruikt waarop je zelf nauwelijks zicht of controle hebt. Bij rekeningrijden krijgt iedere auto een apart kastje dat via GPS precies bijhoudt waar de auto rijdt. Er zijn ruwweg twee architecturen mogelijk: het kastje stuurt die gegevens direct door naar een centrale backoffice waar men op grond van het gereden traject een rekening opstelt. Daartegenover kan zo'n kastje de gegevens ook lokaal houden en zelf de rekening bepalen (of alleen geaggregeerde gegevens aan het centrale niveau doorgeven).
Het centrale beheer van (persoons)gegevens maakt het leven makkelijker. De gebruiker hoeft zelf niks meer te beheren, behalve de authenticatiemiddelen om door de infrastructuur herkend te worden: het individu wordt gereduceerd tot authenticator. Echter, ook hier geldt dat dit centrale beheer een prijs heeft, in termen van verlies van controle en privacy, en van risico's. De ‘machtige partijen’ zijn maar al

te graag bereid om onze gegevens te beheren omdat ze de waarde ervan kennen: ze kunnen er hun betweterige ‘diensten’ mee verbeteren. Vaak is die betweterigheid ook prettig en goed afgestemd. Het is echter belangrijk te beseffen dat er een expliciete keuze is, zoals bij rekeningrijden, om gegevens centraal of decentraal te organiseren. Ook hier geldt weer dat de informatiestromen de machtsverhoudingen bepalen.

Bits en bommen

Hierboven kwam reeds aan de orde dat internet het individu veel nieuwe ontplooiingsmogelijkheden biedt. Dat geldt ook in negatieve zin. Het is voor iemand in Oost-Europa of West-Afrika met een internetaansluiting aantrekkelijker en makkelijker een slecht beveiligde of slordige westerling op afstand op te lichten, dan met een afgezaagd geweer een lokale bank binnen te lopen. Sterker nog, een kwaadaardig individu met de juiste vaardigheden kan hier of aan de andere kant van de wereld een destructief effect hebben dat tot voor kort aan traditionele ‘kinetische’ oorlogsvoering voorbehouden was. Bij het ontwerp van onze ICT-infrastructuur is daar nauwelijks aandacht aan geschonken. Cyberspace vormt een steeds belangrijkere arena voor het uitvechten van geschillen en conflicten, waarbij koppelingen tussen handeling en plaats of tussen handeling en dader minder vanzelfsprekend zijn.

Tot slot

Een gemene deler bij veel van de hierboven geschetste ontwikkelingen is dat individuen enerzijds machtiger lijken te zijn geworden, in termen van ontplooiing en makkelijk beschikbare diensten. Anderzijds is daarbij op de achtergrond de werkelijke macht komen te liggen bij degenen die de informatiestromen en kanalen beheersen. Een beetje cynisch gesteld is het internet bedwelmende opium voor het volk: een iPod geeft je allerlei mogelijkheden maar ketent jou en al jouw gegevens aan de producent die jouw doen en laten volgt, en gebruikt. Het depolitiserende platte amusement van de massamedia is ‘bedwelming 1.0’ en heeft plaatsgemaakt voor gepersonaliseerde beïnvloeding, als ‘bedwelming 2.0’. Zolang de illusie van zelfontplooiing en vrijheid gehandhaafd kan worden, blijven de onderliggende machtsstructuren onaangetast. Manipulatie en disciplinering is van alle tijden, maar de uitoefening ervan is subtieler en minder transparant dan ooit. Het is een lastige vraag in hoeverre de burger hiertegen beschermd wil of moet worden.
Wat betekent dit alles nu voor het landsbestuur? De overheid is natuurlijk niet de ontwerper van de

nieuwe technologieën. Maar de overheid schept wel het wettelijke kader waarin deze technologieën functioneren. Een kaderstellende rol is daarmee de meest natuurlijke. Daarbij verdient een tweetal aspecten aandacht. Allereerst dient de veiligheid en beveiliging van gegevens in de ICT-infrastructuur op een hoger niveau te komen. Daartoe kan een juiste mix van wettelijke verplichtingen, boetes, economische prikkels en bewustwordingscampagnes worden ingezet. Deze verbeterde beveiliging zal de maatschappelijke en persoonlijke kwetsbaarheid verkleinen. Daarnaast: onze democratie is gebaseerd op het beeld van vrije autonome burgers. Het opereren van de hedendaagse informatiegiganten zet dit beeld onder druk. Vrije, onbespiede en ongefilterde toegang tot informatie verdwijnt sluipenderwijs. Dat is misschien wel de grootste uitdaging. Laten we het gebeuren, of zoeken we manieren om er paal en perk aan te stellen?

Literatuur

Agre, P.H., & M. Rotenberg, M. (1997). *Technology and privacy: The new landscape*. Cambridge, MA: MIT Press.

Buruma, Y. (2011). Het recht op vergetelheid. Politiële en justitiële gegevens in een digitale wereld. In D. Broeders, C.M.K.C. Cuijpers & J.E.J. Prins (Red.), *De staat van informatie*, WRR verkenning, 25. (pp.165-221). Amsterdam: Amsterdam Universtity Press.

Jacobs, B. (2011). Autonomie en *transparantie*. In M. Kowalski & M. Meeder (Red.), *Contraterrorisme en ethiek* (pp.56-68). Amsterdam: Boom.

Mayer-Schönberger, V. (2009). *Delete. The virtue of forgetting in the digital age*. Princeton, New Jersey: Princeton University Press.

Morozov, E. (2011). *The net delusion. The dark side of Internet freedom*. New York: Public Affairs..

Pariser, E. (2010). *The filter bubble*. New York: Viking Press.

Staatscommissie Grondwet (2010). *Rapport van de Staatscommissie Grondwet*.

http//:www.staatscommissiegrondwet.nl