GEMEDIEERD VERTROUWEN IN DE OVERHEID
Een wijsgerig-antropologisch perspectief op veiligheid en vertrouwen

Jos de Mul

In zijn *Visiebrief digitale overheid* van 23 mei 2013 heeft de minister van Binnenlandse Zaken en Koninkrijksrelaties aangegeven dat de burger in 2017 al zijn zaken met de overheid via internet moet kunnen regelen. Uit het in december 2013 gepubliceerde onderzoeksrapport *De burger gaat digitaal* stelt de Nationale ombudsman dat een meerderheid van de burgers in ons land dat streven ondersteunt. Dat is niet zo gek, aangezien zij in hun rol als consument reeds massaal zijn overgestapt op online winkelen, het via het internet regelen van bankzaken, het doen van boekingen van vakantiereizen etc. Digitale dienstverlening door de overheid is om dezelfde redenen aantrekkelijk: zij is 24 uur per dag beschikbaar, belooft een forse tijdsbesparing op te leveren en de zaken kunnen bovendien comfortabel vanuit de huiskamer worden geregeld.

De enquête, die de Nationale ombudsman in samenwerking met het consumentenprogramma TROS Radar uitzette, en waarop door ruim 48.000 burgers werd gereageerd, leert evenwel dat de burger in weerwil van deze positieve grondhouding opvallend weinig vertrouwen heeft in de deugdelijkheid van de digitale dienstverlening van de overheid. Bijna de helft heeft geen fiducie in de veiligheid van de ICT-systemen van de overheid, ruim een derde heeft geen vertrouwen in de manier waarop de overheid met de gegevens omgaat, en bijna een vijfde van de respondenten geeft aan wel eens met verkeerde gegevens in overheidssystemen te hebben gestaan. Op een schaal van tien scoort geen enkele overheidsinstantie op het vlak van de digitale dienstverlening hoger dan een mager zeventje (de RWD doet het nog het best met een 6,9), terwijl bijna een kwart een onvoldoende krijgt (waarbij de UWV met een 4,8 het slechtste rapportcijfer krijgt). Deze lage waardering brengt de Nationale ombudsman ertoe de overheid op te roepen gerichte actie te ondernemen om het vertrouwen in de digitale overheid te versterken.[1]

Dat is natuurlijk gemakkelijker gezegd dan gedaan. Met dit essay beoog ik een bijdrage te leveren aan de ontwikkeling van een meer betrouwbare digitale overheid door de op het eerste gezicht paradoxale tegenstelling tussen enerzijds de bereidheid van de burger ‘digitaal te gaan’ en anderzijds diens gebrek aan vertrouwen in de digitale dienstverlening van de overheid aan een nadere analyse te onderwerpen. Ik zal betogen dat deze paradox samenhangt met het sterk gemedieerde karakter dat het vertrouwen in de informatiesamenleving heeft gekregen. Waar in de traditionele gemeenschap vertrouwen vooraleerst een interpersoonlijk karakter bezat, en in de moderne staat de gestalte aannam van een meer afstandelijk systeemvertrouwen, daar wordt het vertrouwen in de informatiesamenleving in toenemende mate gemedieerd door voor de burger onzichtbaar functionerende informatietechnologieën, waarvan de effecten het vertrouwen in de digitale overheid van binnenuit dreigen uit te hollen.

Teneinde deze stelling te onderbouwen, zal ik in het eerste deel van het essay stilstaan bij de betekenis van de begrippen ‘veiligheid’ en ‘vertrouwen’ en een aantal aanverwante noties. In het tweede deel zal ik een aantal kenmerken van de informatiesamenleving

beschrijven die betrekking hebben op het vertrouwen, om vervolgens in het derde deel in te gaan op de uitdagingen én kansen die het gemedieerde vertrouwen met zich meebrengt voor een overheid die het vertrouwen van de burger in haar digitale dienstverlening wil versterken of terugwinnen.

Velerlei vertrouwen

Het menselijk leven is bijzonder kwetsbaar. Als baby zijn we volstrekt afhankelijk van de zorg van volwassenen, zonder zuurstof, water en voedsel sterven we binnen een korte tijdspanne en zelfs wanneer in deze primaire levensbehoeften wordt voorzien, wordt onze veiligheid op talloze manieren bedreigd. Natuurgeweld, ziekten, ongelukken, misdaden en oorlogen dreigen voortdurend ons leven en levensgeluk te ondermijnen. In zijn boek *Leviathan* (1651) schetst de Britse filosoof Thomas Hobbes bij wijze van gedachtenexperiment een afschrikwekkend beeld van het leven van de mens in de natuurtoestand: “no account of Time; no Arts; no Letters; no Society; and which is worst of all, continual fear, and danger of violent death: And the life of man, solitary, poor, nasty, brutish and short.”[2]

Het beeld dat Hobbes van de natuurtoestand van de mens schetst is waarschijnlijk wat al te somber. Volgens huidige inzichten leefde de prehistorische jager-verzamelaar in kleine groepen, waarbinnen weliswaar concurrentie om voedsel en partners bestond, maar waarin de stamleden ook intensief samenwerkten bij de jacht en in de strijd tegen andere stammen, óók voedsel deelden, voor elkaar zorgden en elkaar beschermden.[3] De mens bezit zeker egoïstische en gewelddadige trekken, maar is ook een sociaal wezen dat zijn leven samen met anderen leeft en daarbij veiligheid schenkt en ontvangt. De dagelijkse berichten over de vele (burger)oorlogen en gewelddadige onderdrukking op vele plaatsen op aarde maken echter duidelijk dat de barbarij en despotische heerschappij waarover Hobbes spreekt, geen louter prehistorisch verschijnsel is, maar een mogelijkheid die inherent is aan de menselijke levensvorm en die zich altijd opnieuw kan voltrekken. En hoewel Nederland al ruim zeventig jaar verschoond is gebleven van oorlogsgeweld binnen haar grenzen, zijn ziekten, ongelukken, misdaden en natuurgeweld voor ons, niet minder dan voor de prehistorische mens, toevalligheden die ons leven en levensgeluk bedreigen.

In de loop van de cultuurgeschiedenis heeft de mens allerlei strategieën beproefd om de fatale toevalligheden die het leven bedreigen te domesticeren.[4] Teneinde de oorlog ‘van allen tegen allen’ te voorkomen, zo merkt Hobbes in *Leviathan* op, hebben individuen geleerd zich te onderwerpen aan een soevereine vorst, die het monopolie op geweld en belastingheffing kreeg toegewezen, wat hem in staat stelde de veiligheid van allen te garanderen. In een moderne democratische rechtstaat zoals Nederland ligt soevereiniteit niet langer bij een absoluut heerser, maar bij het volk zelf. Het doel, de veiligheid van allen te garanderen, is evenwel hetzelfde gebleven. De moderne wetenschap en technologie stellen ons bovendien in staat op talloze dimensies van het leven het lot in eigen hand te nemen: dankzij de geneeskunde kunnen veel ziekten tegenwoordig worden voorkomen en genezen, dijken beschermen ons tegen het geweld van de Noordzee, en de overheid zet uiteenlopende technologische middelen in om de veiligheid van het voedsel, de werkvloer, de openbare ruimte etc. te garanderen en criminaliteit en terrorisme te bestrijden.

Basaal vertrouwen

In alle strategieën om het toeval te domesticeren, speelt vertrouwen een cruciale rol. Vertrouwen betekent leven *alsof* er geen fatale toevalligheden in het leven bestaan. Vertrouwen ontkent in meer of mindere mate het bestaan van dergelijke toevalligheden en biedt als zodanig gemoedrust. Gemoedsrust, maar geen garanties. Vertrouwen heeft immers betrekking op een toekomst die fundamenteel onkenbaar en onzeker is.

Daarbij kunnen we verschillende vormen van vertrouwen onderscheiden. Om te kunnen leven is er in de eerste plaats een *basaal vertrouwen* nodig in de wereld om je heen, je medemensen en jezelf. We gaan er doorgaans vanuit dat de wereld morgen aan dezelfde natuurwetten onderhevig is als vandaag, dat de regels van het sociale verkeer niet plotsklaps veranderen, en dat ook ikzelf morgen nog grotendeels dezelfde persoon zal zijn gebleven. In een onbegrijpelijke of permanent veranderende wereld kan vertrouwen niet tot stand komen. We mogen er vanuit gaan dat ook de prehistorische mens deze vorm van vertrouwen, zonder welke geen gemeenschap mogelijk is, reeds kende.

Het verkrijgen van dit basaal vertrouwen start al in het vroegste stadium van het leven. Kinderen vertrouwen er blindelings op dat hun ouders hen te eten zullen geven en beschermen. Deze door psychologen als *basic trust* aangeduide vorm van vertrouwen ligt ten grondslag aan alle latere vormen van vertrouwen. Langzaam bouwt dit zich vervolgens uit naar situaties en mensen die zich buiten de vertrouwdheid van het eigen gezin bevinden.

Hoewel robuust, biedt zelfs basaal vertrouwen geen garanties. Sommige ouders verwaarlozen hun kinderen, partners en vrienden zijn soms ontrouw, en we kunnen onszelf verliezen in onvermoede passies. Die onvoorspelbaarheid van het menselijk handelen is eigen aan de vrijheid van de mens. Kenmerkend voor het basaal vertrouwen is evenwel dat het vanwege zijn blind karakter zelfs wanneer het wordt beschaamd, vaak nog standhoudt. Kinderen en bedrogen geliefden blijven vaak tegen beter weten in vertrouwen in de ander behouden, en we blijven meestal ook geloven in ons zelf, zelfs wanneer we onszelf ontrouw zijn. Veranderingen gaan dikwijls tergend langzaam omdat het houvast dat door gewoonten en vigerende normen geboden wordt – ook als ze in conflict zijn met ons intellectuele of morele kompas - maar moeilijk los te laten is. Pas wanneer het basaal vertrouwen te ernstig en/of te vaak wordt beschaamd, gaat het verloren en kan het zelfs omslaan in zijn tegendeel. Dan neemt een fundamenteel wantrouwen tegenover de wereld zijn plaats in.

Interpersoonlijk vertrouwen

Naast dit basale vertrouwen, bestaat er ook een *interpersoonlijk vertrouwen*, dat eigen is aan de kleine leefgemeenschap en zich afspeelt tussen personen. Interpersoonlijk vertrouwen is, anders dan basaal vertrouwen, geen vanzelfsprekendheid, maar is gebaseerd op ervaring. In kleine gemeenschappen betreft het vaak *gezamenlijke ervaringen* die persoonlijk vertrouwen mogelijk maken – iedereen gaat naar dezelfde kerk, jeugdbeweging of speelt in hetzelfde hockeyteam.

Maar ook tussen personen die verder van elkaar afstaan is interpersoonlijk vertrouwen mogelijk. Omdat de groenten en het fruit bij de groenteboer om de hoek tot nu toe altijd van

uitstekende kwaliteit zijn geweest, gaan we er vanuit dat dit ook vandaag weer het geval zal zijn. Interpersoonlijk vertrouwen is minder diep verankerd dan de van kindsbeen af opgebouwde vertrouwdheid. We zijn ons hier ook meer bewust van de risico's en handelen daar ook naar. We kijken eerst de kat uit de boom. We laten de aannemer eerst een klein klusje uitvoeren, voordat we hem ons hele huis laten verbouwen. En wanneer hij ons vertrouwen beschaamd, gaan we bij de volgende gelegenheid met een andere aannemer in zee.

Systeemvertrouwen

In de moderne, industriële samenleving, die gepaard is gegaan met de ontwikkeling van complexe maatschappelijke instituties en infrastructuren, is een derde vorm van vertrouwen ontstaan, dat we met Luhmann kunnen aanduiden als *systeemvertrouwen*.[5] Waar de eerder besproken vormen van vertrouwen doorgaans zijn verbonden aan een bepaalde locatie, daar heeft systeemvertrouwen betrekking op omvangrijke, nationaal of zelfs internationaal functionerende systemen en instituties. Voorbeelden daarvan zijn de luchtvaart, het geldverkeer en (inter)nationale overheden. Hun functioneren is afhankelijk van veelal anonieme experts. Dat betekent overigens niet dat interpersoonlijk vertrouwen hier geen enkele rol speelt. Tussen de abstracte systemen en de gebruikers staat de functionaris – de piloot, bankier, ambtenaar, agent etc. - die een cruciale rol speelt bij het al of niet tot stand komen of in stand houden van het systeemvertrouwen.[6]

Net als bij het basaal vertrouwen en interpersoonlijk vertrouwen is ook het systeemvertrouwen niet vrij van risico's. Omdat die complexe en daardoor kwetsbare systemen en instituties alomtegenwoordig zijn in de moderne maatschappij, wordt deze door sociologen als Beck en Giddens ook wel aangeduid als een risicosamenleving.[7] Toch zijn we ons vaak minder dan bij interpersoonlijke relaties bewust van die risico's. Zolang het systeem functioneert, wordt het – net als in het geval van basaal vertrouwen – min of meer als vanzelfsprekend gezien. Pas wanneer het systeem 'crasht' - zoals dat bijvoorbeeld gebeurde bij het faillissement van de internetspaarbank Icesafe en bij het neerhalen van de MH17 – worden we ons (weer) van de risico's bewust. Een ander belangrijk verschil tussen interpersoonlijk vertrouwen en systeemvertrouwen is dat we, wanneer het vertrouwen wordt beschaamd, het in het eerste geval vooral aan onze eigen goedgelovigheid wijten, terwijl we in het geval van een systeemcrash de beschuldigende vinger eerder naar de verantwoordelijke beheerders van het systeem wijzen.[8] En dat is in de laatste instantie vaak de overheid, wier belangrijkste taak het immers is over onze veiligheid te waken. Zeker in een samenleving zich in sneltreintempo tot een informatiesamenleving ontwikkelt, is dat geen sinecure.

Leven in de informatiesamenleving

Sinds enkele decennia tekent zich een wereldwijde ontwikkeling af, die – als opvolger van de Agrarische Revolutie en de Industriële Revolutie - wel wordt aangeduid als de derde grote omwenteling in de geschiedenis van de mensheid: de Informationele Revolutie.[9] Waar de agrarische samenleving draaide om het bezit van *materie* (land ten behoeve van landbouw en veeteelt), en de industriële samenleving om de productie en het beheer van *energie* (waarvoor niet zozeer land als wel machines en dus kapitaal vereist zijn), daar draait het in de

informatiesamenleving steeds meer om de productie, het beheer en de communicatie van *informatie*. Informatie- en communicatietechnologieën (ICTs) vormen het zenuwstelsel van onze huidige samenleving en hebben geleid tot een nieuwe fundamentele transformatie van maatschappelijke organisatiestructuren, machtsrelaties en technologische beheersing.[10] Of het nu gaat om de economie, wetenschap, publieke ruimte, politiek, recht, defensie, of de dienstverlening door de overheid, niets wordt onberoerd gelaten door de alom tegenwoordige informatietechnologie.

De fundamentele informatisering van natuur en cultuur raakt ook en op ingrijpende wijze ons wereld- en mensbeeld. Waar in het tijdvak van de Industriële Revolutie de wereld en de mens werden begrepen als een ingewikkeld mechanisme – het heelal als klok, het hart als pomp – daar domineren in de informatiesamenleving computermetaforen. Het heelal, de hersenen, en de individuele cel worden nu steeds vaker in termen van informatieverwerking begrepen. Naast materie en energie lijkt informatie een fundamentele bouwsteen van het universum te zijn.[11]

Online leven

Door de introductie van steeds kleinere en intiemere ICTs - pc, laptop, navigatiesysteem, tablet, smartphone, smartwatch, elektronische implantaten – verstrengelt ook ons dagelijks leven zich onlosmakelijk met informatietechnologieën. Persoonlijke relaties, beroepen, koopgedrag en vrije tijd zijn door het World Wide Web, sociale media en apps onherkenbaar veranderd. Ons leven offline en online versmelt tot een hybride *onlife* leven.[12] De in rap tempo voortschrijdende *dataficatie* van dingen, personen en gebeurtenissen transformeert onze wereld tot een 'Internet of Everything'.[13] Of het nu gaat om het assortiment van een webwinkel, de trillingen van de brug, het genoom van de E. coli bacterie, of om de persoonsgegevens van een individu en diens koopgedrag, mobiliteit, zoekacties op Google en interacties op Twitter en Facebook, door de koppeling van de vele relationele, transactionele, geografische, ruimtelijke en beslissings-ondersteunende databases ontstaat een gigantische 'datawolk', die de belangrijkste grondstof van de informatiemaatschappij vormt. Deze Big Data lenen zich voor uiteenlopende vormen van *datamining* en *profiling*. Deze 'datascope' is de nieuwe telescoop en microscoop waarmee we verder en dieper in de natuur en de menselijke samenleving kunnen kijken.[14]

Datamining en profiling

Het succes van het Web 2.0 berust op de combinatie van gebruikers en kunstmatige intelligentie, die leidt tot een collectieve intelligentie, die wel wordt aangeduid als *the wisdom of the crowds* of 'zwermgeest'.[15] De door de gebruikers aan de 'voorzijde' van de website ingevoerde data worden aan de achterzijde - onzichtbaar voor de gebruikers - opgeslagen in een 'relationele database', en kunnen vervolgens met behulp van *datamining* op interessante patronen worden doorzocht, gerecombineerd, en gekoppeld aan andere databases. De consument vult de database van Amazon.com en Bol.com met zijn of haar persoonsgegevens, locatie, koopgedrag, waardering van de gekochte waren, reviews etc. Die 'dataschaduw' wordt met behulp van *item-to-item filtering* door Amazon geanalyseerd en gekoppeld aan de data van

andere kopers, waardoor het bedrijf allerlei voorspellingen kan doen over toekomstige aankopen (waar, wanneer, door wie etc.). Daardoor weet Amazon al, voordat de koper daar zelf achter komt, welk boek hij of zij in de toekomst zal willen lezen. In december 2013 verkreeg het bedrijf zelfs een patent op 'anticipatory shipping'.[16] Met behulp van *profiling* technieken wordt die kennis vervolgens gebruikt om iedere klant een volstrekt geïndividualiseerde website met passende aanbevelingen en reclames voor te schotelen. Dat werkt bijzonder effectief. Waar het bedrijf aanvankelijk een heleboel mensen in dienst had om aanbevelingen bij de koopwaar te schrijven, werden die massaal ontslagen na de introductie van het genoemde *item-to-item filtering* algoritme, niet alleen omdat dit goedkoper is, maar het is ook vele malen succesvoller dan zijn menselijke evenknie. Amazon genereert hiermee nu reeds meer dan een derde van haar omzet.[17] Niet alleen de online shop van Amazon, de zoekmachines van Google en sociale media sites als die van Facebook en Twitter maken gebruik van *datamining* en *profiling*, maar ook banken en verzekeraars doen dat, evenals hackers en criminelen. En ook de overheid blijft bij dit alles niet achter.

De dubbelzinnige rol van de overheid in de informatiesamenleving

De positie van de overheid in de informatiemaatschappij is echter dubbelzinnig.[18] Enerzijds dient zij vanwege haar verantwoordelijkheid voor de maatschappelijke infrastructuren de veiligheid en betrouwbaarheid van de informatienetwerken te garanderen. Omdat deze het zenuwstelsel van de informatiesamenleving vormen is dat van fundamenteel belang. Maar gezien het internationale en private karakter van grote delen van het internet (Google, Facebook) en de permanente innovatie die de ICT kenmerkt, is dat een lastige en niet zelden zelfs onmogelijke taak. Anderzijds maakt de overheid ook zelf gebruik van de informationele infrastructuur. Niet alleen om de informatieverschaffing en dienstverlening te verbeteren, maar juist ook om haar veiligheidstaken met betrekking tot het internet, maar ook daarbuiten, te realiseren. Bijvoorbeeld door *datamining* en *profiling* te gebruiken om netwerken van actuele of potentiële verspreiders van kinderpornografie of terroristen in kaart te brengen en individuele daders te kunnen oppakken.

De wet van de onbeheersbare complexificatie

Gezien de toename van de complexiteit van de informatiemaatschappij is de inzet van ICTs voor zulke taken onvermijdelijk. Zoals de toename van de maatschappelijke complexiteit in de agrarische samenleving aan de wieg stond van de uitvinding van het schrift (dat zijn oorsprong vond in het registreren van voedselvoorraden en handelsstromen), en de nog veel grotere complexiteit van de industriële samenleving noopte tot een omvangrijke, door de drukpers mogelijk geworden documentatie, zo valt de informationele complexiteit van de huidige samenleving niet langer te doorgronden en beheersen zonder de massale inzet van computers. Zowel de *hoeveelheid* informatie (dagelijks wordt er een hoeveelheid data aan het internet toegevoegd die gelijk is aan een stapel dvd's van de aarde naar de maan en terug!) als de *exponentiële toename* van die hoeveelheid data (iedere twee jaar verdubbelt de totale hoeveelheid) vormt een probleem. Bovendien neemt ook de *complexiteit* van de datawolk exponentieel toe, wat leidt tot combinatorische explosies. De hoeveelheid mogelijk

(re)combinaties van geatomiseerde data tart de menselijke verbeelding en maakt het onvermijdelijk na het geheugen ook de analytische vermogens van de mens uit te besteden aan de computer, hoewel zelfs die daar vaak machteloos tegenover staat.[19]

Net als het schrift en de boekdrukkunst dreigt de informatietechnologie onder haar eigen succes te bezwijken. Zeker sinds de uitvinding van de boekdrukkunst is er een onoverzichtelijke informatieberg ontstaan. Waar de collectie van de beroemde bibliotheek van Alexandrië in de Oudheid bestond uit ongeveer 4000 handschriften, daar had de British Library in 2013 een collectie van ongeveer 170 miljoen boeken en overige items, en daar zijn de afgelopen twee jaar alleen al ca. 3 miljoen wetenschappelijke publicaties bijgekomen. Op een vergelijkbare manier creëert de inzet van geavanceerde ICTs om complexiteit te bedwingen onvermijdelijk een nog veel grotere complexiteit. We kunnen dieper dan ooit ingrijpen in de elementaire structuren van de levenloze en levende natuur - denk aan nanotechnologie en op de genetica gebaseerde biotechnologie - en van het informationele zenuwstelsel van de samenleving, maar dat betekent niet dat we deze structuren ook volledig beheersen. De opeenvolgende financiële crises die de wereld sinds 2008 in hun greep houden, zijn een goed voorbeeld van deze 'wet van de onbeheersbare complexificatie'. Zij zijn niet alleen te wijten aan de combinatie van *greedy* bankiers en perverse prikkels, maar ook aan het feit dat zelfs de briljantste ontwerpers van deze complexe financiële producten de – naar al spoedig bleek fatale - neveneffecten daarvan niet konden voorzien.[20]

Een optocht van misverstanden en fouten

Ook grootschalige ICT-projecten bij de overheid lopen nogal eens mis vanwege de onderschatte complexiteit. In zijn rapport *Lessen uit ICT-projecten bij de overheid* merkte de Algemene Rekenkamer in 2008 op dat ICT-projecten bij de overheid doorgaans veel duurder blijken uit te vallen dan verwacht, veel meer tijd vergen dan gepland en bovendien vaak niet het gewenste resultaat opleveren.[21] Heel veel lijkt de overheid niet te hebben geleerd van dat rapport, want sindsdien lijkt het aantal mislukte ICT-projecten van de overheid slechts in aantal en omvang te zijn toegenomen, getuige het ruim 200 miljoen kostende, maar nooit functionerende computersysteem ETPM van de Belastingdienst, waar in 2014 de stekker uit werd getrokken,[22] en het in mei 2015 gesneefde SPEER (inmiddels omgedoopt tot ERP), volgens de Algemene Rekenkamer met bijna 900 miljoen euro het duurste ICT-project van de Nederlandse overheid ooit.[23] De belangrijkste oorzaak van deze "optocht van misverstanden en fouten" is volgens de Algemene Rekenkamer "dat ICT-projecten van de overheid vaak te ambitieus en te complex worden door de combinatie van politieke, organisatorische en technische factoren. Bij deze al te complexe projecten is er geen balans tussen ambitie, beschikbare mensen, middelen en tijd".[24]

Het systeemvertrouwen in de overheid neemt door (de media-aandacht voor) dergelijke grootschalige mislukkingen natuurlijk niet toe. Temeer omdat dat vertrouwen bij deze projecten vaak ook nog om een andere reden wordt beschaamd. In het eveneens uit 2008 daterend, maar sindsdien alleen maar relevanter geworden rapport *Informatie: grondstof met toekomstwaarde*, concludeerden de Raad voor het Openbaar Bestuur en de Raad voor Cultuur: "Een goede en betrouwbare informatiehuishouding is van vitaal belang voor de overheid.

Politiek en ambtelijk management gaan echter tamelijk zorgeloos met dit belang om. De aandacht voor een ordentelijke informatiehuishouding schiet structureel te kort. Dit is een oud probleem dat verregaand versterkt wordt door de voortschrijdende digitalisering. Doorgaan op dezelfde weg betekent onvermijdelijk de aantasting van belangrijke rechtsstatelijke waarden zoals transparantie, zorgvuldigheid, toegankelijkheid, verantwoording en verantwoordelijkheid".[25] Na de onthullingen van WikiLeaks en Snowden is duidelijk geworden dat er naast de gesignaleerde zorgeloosheid soms ook sprake is van opzettelijke aantasting van die rechtstatelijke waarden. Daarmee wordt de weg ingeslagen die loopt van systematisch wantrouwen naar meer of minder paranoïde complottheorieën.

Wat het vertrouwen in de overheid de afgelopen decennia bovendien heeft ondermijnd is het feit dat overheden ICT's tot op heden vooral hebben ingezet ter ondersteuning van hun eigen taken en in veel mindere mate ter ondersteuning van de activiteiten van hun burgers.[26] De digitale belastingaangifte was jarenlang een van de weinige positieve uitzonderingen.[27] Daarom zien we dat burgers in de informatiesamenleving met de hulp van het internet en de sociale media het heft in eigen hand nemen.[28] Zij zijn vaak goed geïnformeerd, alert en assertief, en niet zelden beter geëquipeerd dan de op het gebied van ICT-innovatie vaak toch wat na-ijlende overheid. Bovendien is door de op het internet overvloedig beschikbare (maar vaak ook tegenstrijdige) informatie de autoriteit van artsen, wetenschappers, en gezagdragers niet langer een gegeven. Ook overheidsfunctionarissen worden regelmatig via de sociale media ter verantwoording geroepen en kunnen niet meer zo gemakkelijk meer wegvluchten in de achterkamertjes van de bureaucratie.

Onder invloed van (neoliberale) deregularisering en privatisering verschuiven bovendien steeds meer publieke taken naar de private sfeer. Tegelijkertijd hebben zelforganisatie, mobilisering, participatie en activisme in de informatiesamenleving een geheel nieuwe dimensie gekregen (de zogenaamde doedemocratie). Door de kleinschaligheid lijkt er hier sprake te zijn van een door ICTs gemedieerde herleving van het persoonlijk vertrouwen. Of we deze ontwikkeling nu zien als een veeg teken van de afbraak van de verzorgingsstaat, zoals dat aan de linker zijde van het politieke spectrum gebeurt, of haar, met conservatieven als de onlangs herkozen Engelse minister-president Cameron, juist opvatten als een stap op weg naar een zelfverantwoordelijke Big Society (waardoor de overheid een paar stappen kan terugtreden), duidelijk is dat de relatie tussen overheid en burger hierdoor fundamenteel verandert.

Digitale kansen voor de overheid

Hier liggen voor de overheid ook kansen. Het Web 2.0 model dat zijn commerciële succes inmiddels genoegzaam heeft bewezen, zou ook door de overheid meer dan tot nu toe gebruikelijk is, kunnen worden ingezet. De publieke zaak zou zo meer een co-creatie van overheid en burgers worden. In het licht van de volkssoevereiniteit is dat ook helemaal niet zo'n gek idee. 'De overheid? Dat zijn wij!' De hoop die daarmee verbonden is, behelst dat de *Overheid 2.0* haar taken niet alleen goedkoper, maar ook efficiënter en effectiever kan uitvoeren.[29]

Tussen droom en daad staan echter ook hier (privacy) wetten en praktische bezwaren in

de weg. In dit essay beperk ik me tot het in de inleiding gesignaleerde probleem van het geslonken vertrouwen in de 'digitale overheid' en zal ik enkele voorwaarden schetsen die het vertrouwen weer zouden kunnen herstellen. Maar voordat ik dat doe wil ik nog een moment stilstaan bij het feit dat dit verlies in vertrouwen niet beperkt is tot de overheid, maar de afgelopen jaren ook is gegroeid met betrekking tot de markt. Behalve door de kwalijke praktijken van de banken (woekerpolissen, investeringen in rommelhypotheken en andere ondoorzichtige financiële producten) en de opkomst van internetcriminaliteit (*fishing*, inbraak in computers, identiteitsdiefstal) is die afname van vertrouwen ook veroorzaakt door het herhaaldelijk in opspraak komen van multinationals als Google en Facebook. Dat heeft niet alleen van doen met de vele privacy-schendingen, maar ook met het machtsverschil en de economische wanverhouding tussen die bedrijven en hun klanten. ICT-gebruikers zijn weliswaar nog altijd bereid met hun data te betalen voor de 'gratis' diensten die genoemde bedrijven leveren, maar zij storen zich aan het feit dat zij nauwelijks inzicht hebben in wat er met hun data gebeurt. En in de gevallen dat ze daar, vaak dankzij hackers of onafhankelijke onderzoekers, wel van op de hoogte zijn, blijkt vaak dat zij als prod*users* (typo intended!) van de waardevolle grondstoffen daarvoor maar een schamel loon ontvangen.

Dat heeft de afgelopen jaren binnen het economisch domein geleid tot allerlei bottom-up initiatieven, zoals crowd funding, micro-kredieten, P2P leningen etc. Activisten zoals Jeron Lanier in zijn *Who ownes the future?* pleiten zelfs voor een radicale herstructurering van het web, die het mogelijk moet maken dat bedrijven als Google en Facebook hun prod*users* per klik voor hun data gaan betalen.[30] Hierin ligt denk ik ook een belangrijke les voor de overheid. Zoals *consumenten* in toenemende mate zeggenschap opeisen m.b.t. het commerciële machtsmisbruik van hun data door marktpartijen, kan worden verwacht dat zij in hun rol van *burger* in de *onlife society* in ruil voor hun data en participatie steeds vaker zeggenschap zullen gaan opeisen om politiek misbruik daarvan te voorkomen. Wanneer de door de burgers aan de overheid verschafte data worden gebruikt op een manier die ten goede komt aan hun individuele en/of collectieve welzijn, dan lijken de meeste burgers daar ook in dit domein weinig op tegen te hebben. Mits ze er op kunnen vertrouwen dat er recht wordt gedaan aan belangrijke rechtsstatelijke waarden, zoals de eerder genoemde transparantie, zorgvuldigheid, toegankelijkheid, verantwoording en verantwoordelijkheid.[31] Maar het probleem is, zoals opgemerkt, dat dit vertrouwen juist onder druk staat.

De digitale overheid: vertrouwdheid, vertrouwen en trouw

Hoe kan de overheid het vertrouwen van haar *onlife* burgers zodanig herstellen dat deze bereid blijven om op grote schaal digitale publieke diensten af te nemen en om onbezoldigd in dienst van de overheid te treden en als prod*users* van data de publieke zaak te dienen? Om die vraag te beantwoorden zal ik achtereenvolgens nog wat dieper ingaan op drie aspecten van vertrouwen die in de informatiemaatschappij op een nieuwe wijze worden uitgedaagd: vertrouwdheid, betrouwbaarheid en trouw.

Organismen zijn altijd omgeven door een – het woord zegt het al – omgeving. Ze kunnen niet zonder, ze zijn er van afhankelijk om te kunnen leven. Dat geldt voor de mens niet minder dan voor de simpelste bacterie. Maar de omgeving is ook een bron van mogelijk gevaar

en potentieel onveilig. Daarom is de cel omgeven door een semipermeabel membraan. Dat stelt hem niet alleen in staat om op selectieve voedingstoffen op te nemen en afvalstoffen uit te stoten, maar het helpt hem ook de voor het leven onontbeerlijke stoffen 'veilig' binnen te houden en kwalijke substanties 'buiten de deur' te houden. Membranen vinden we niet alleen bij de cel, maar ook op de daaropvolgende vitale aggregatieniveaus van het leven: van de weefsels die de organen beschermen en de huid die het dier omhult, tot aan huizen, hekken rondom tuinen, stadsmuren en landsgrenzen die de menselijke cultuur kenmerken. En ook in de virtuele wereld treffen we ze aan in de vorm van firewalls, en zogenaamde "online walled gardens" zoals Facebook en smartphone-apps. Ze verschaffen veiligheid, maar door hun semipermeabele karakter kunnen ze die nooit absoluut garanderen: gifstoffen kunnen het organisme binnendringen, inbrekers ons huis, terroristen ons land, en virussen zijn zowel in de fysieke als de virtuele wereld actief. Leven is nu eenmaal nooit zonder risico's. Maar indien het semipermeabele membraan (meestal) goed functioneert, kunnen we erop vertrouwen dat het ons veiligheid verschaft.

Vertrouwdheid

Het vertrouwen is niet alleen maar afhankelijk van de kwaliteit van de beschermende membraan, maar ook van de *vertrouwdheid* die we hebben met het membraan en de wereld aan gene zijde van het membraan, de omgeving. Voor wie 's avonds laat over straat loopt, zal het gevoel van veiligheid mede afhangen van de bekendheid met de buurt. In een onbekende buurt voelen we ons eerder onveilig dan in een ons bekende buurt. En omdat ik vertrouwd ben met de website van mijn bank, voel ik mij daar veiliger dan wanneer ik een online betaling verricht op de website van een onlineshop die ik voor het eerst bezoek. Het subjectieve gevoel van veiligheid is dus niet altijd gelijk aan de objectieve veiligheid. Het kan zelfs gebeuren dat een objectieve toename van de veiligheid, bijvoorbeeld de afname van criminaliteit in een bepaalde wijk door het ophangen van bewakingscamera's, resulteert in een afname van de subjectief ervaren veiligheid. Waar zoveel camera's hangen, zal het wel niet pluis zijn. Daarnaast beïnvloedt ook de aandacht die in media aan (on)veiligheid wordt geschonken het subjectieve gevoel van veiligheid. Hoewel het CBS in april 2015 voorrekende dat de misdaad al tien jaar daalt en nog nooit zo snel als vorig jaar, voelt één derde van de burgers in Nederland zich onveilig.

Ook in de wondere wereld van de ICTs is het merkwaardig gesteld met het fenomeen vertrouwdheid. Enerzijds doen ontwerpers van websites bijvoorbeeld hun best een vertrouwde indruk te wekken. De sober ogende zoekmachine van Google ziet er, sinds deze bijna twintig jaar geleden op het World Wide Web opdook, nog steeds min of meer hetzelfde uit. Tegelijkertijd verkeert de wereld van de informatietechnologie in een permanente bètastaat. Apparaten, besturings-systemen, software, apps en websites veranderen zo snel dat ze al weer verouderd zijn voordat we er goed en wel vertrouwd mee zijn.

Bovendien is het vaak droevig gesteld met de gebruiksvriendelijkheid, wat ook al niet bijdraagt aan de vertrouwdheid. Het Erasmus Employee Self Service Portal, om een voorbeeld uit eigen ervaring te noemen, drijft zelfs de meest geharde ICT-optimist tot wanhoop. Het declareren van een simpele binnenlandse dienstreis, dat vroeger een paar minuten tijd vergde,

dwingt de medewerker nu een onoverzichtelijk labyrint van menu's te passeren, waar hij of zij al snel een half uur mee zoet is. Maar de overheid kan er ook wat van! De UWV-website Werk.nl scoorde bij een door vakbond FNV uitgevoerde enquête een schamele 2,7: de site vertoont herhaaldelijk storingen, waardoor niet kan worden ingelogd of de site zelfs geheel onbereikbaar is. Het voor systeemvertrouwen zo cruciale persoonlijke contact met een menselijke werkcoach is vanwege bezuinigingen slechts 10% van de werkzoekenden gegund. Door het gebruik van door verschillende bedrijven gemaakte, niet goed op elkaar afgestemde extractie- en matchingprogramma's in de *backend* van de website gaat het ook nogal eens mis met de verstrekte adviezen. Zo kregen bijvoorbeeld begeleiders in de gehandicaptenzorg vacatures in de bouw aangeboden en Nederlandstaligen '100 procent passende' vacatures in het Pools .[32]

Betrouwbaarheid

Net als in het geval van 'traditioneel' systeemvertrouwen, merken we het informatietechnologische systeem meestal pas op, wanneer er iets mis gaat, bijvoorbeeld wanneer een Nederlandse werkzoekende ineens Poolse vacatures in het Pools krijgt aangeboden. Maar zelfs in die gevallen hebben we nauwelijks inzicht in wat zich nu precies aan de achterzijde van de website afspeelt. Vaak is die *backend* voor de gebruiker zelfs een volslagen *black box*. Achter die eenvoudig ogende pagina van Google Search worden de methoden van *datamining* en *profiling* steeds geavanceerder zonder dat we beseffen hoezeer de zoekresultaten daar in belangrijke mate door worden bepaald. Ook de gebruikersinterface is een membraan, tussen de gebruiker van de website en de database die zich daarachter bevindt, maar het is er een die niet alleen de gebruiker 'beschermt' tegen de vaak complexe programmatuur in de *backend* van de website, maar vooral ook de eigenaar van de website, die het te winnen informatiegoud niet graag met anderen deelt. Daardoor is wat bij sociale media als Facebook op het eerste gezicht een interpersoonlijke vertrouwensband tussen gebruikers lijkt te zijn, in sterke mate een door computerprogramma's gemedieerd vertrouwen. Hoewel het lijkt alsof de 'vrienden' spontaan met elkaar in contact komen en een vertrouwensrelatie opbouwen, worden de interacties in sterke mate bepaald door de eigenaar van de website, al was het alleen al doordat de – op commerciële belangen afgestemde - algoritmen van Facebook bepalen welke berichten men überhaupt in de News Feed te zien krijgt.[33] En zelfs wanneer een bedrijf als Facebook, dat om de haverklap de privacy settings verandert, door wetgeving gedwongen de gebruikers een bescheiden kijkje in de 'mijn' gunt, zal vrijwel niemand de tijd vinden en/of de technische en juridische expertise bezitten om de vele tientallen pagina's tellende voorwaarden te doorgronden. Zolang de gebruiker zich niet bewust is van wat er achter het beeldscherm van zijn pc, tablet of smartphone gebeurt, hoeft dat het gevoel van veiligheid en daarmee vertrouwen in aanbieders van de uiteenlopende internetdiensten niet werkelijk te beschamen. Maar door de vele in de pers - terecht - breed uitgemeten schandalen over privacy-schendingen, het onaangekondigd doorverkopen en de diefstal van persoonsgegevens, groeit het gevoel van onveiligheid en daarmee ook het wantrouwen.

Daarbij gaat het om meer dan een gevoel, want ook de feitelijke machtsverhoudingen in

de informatiesamenleving hebben een belangrijke transformatie ondergaan door het digitale zichtbaarheidsregiem. In zijn beroemde studie *Surveiller et punir. Naissance de la prison* betoogt de Franse filosoof Foucault dat zich met de overgang in Europa van het *ancien régime* van de absolute vorst naar de moderne staat een omkering van het zichtbaarheidsregime heeft voltrokken.[34] Waar in het eerste geval de Soeverein zich in al zijn pracht en praal, en niet te vergeten in zijn absolute macht aan het volk toonde, terwijl de onderdanen die zich niet wensten te onderwerpen onzichtbaar wegkwijnden in de kerkers, daar is in de moderne staat de macht onzichtbaar geworden en wordt juist de burger zichtbaar gemaakt door middel van statistisch onderzoek en panoptisch toezicht. Het paradigmatische voorbeeld van het laatstgenoemde is de moderne koepelgevangenis, waarin de gevangenen in hun 'doorzoncellen' door één enkele bewaker in een centrale toren in de gaten kunnen worden gehouden. De kracht van het panoptische model is mede gelegen in het feit dat de gevangenen niet kunnen zien of de bewaker zich daadwerkelijk op zijn post bevindt. Ook wanneer hij er niet is zullen de gevangen zichzelf met zijn blik identificeren en daarmee zichzelf disciplineren. De bewakingscamera, de hedendaagse variant van het Panopticum, bewerkstelligt hetzelfde effect. De potentiële winkeldief waant zich bespied, ook al weet hij niet zeker of de camera wel aan staat en of de beelden worden bekeken. Dat is een *known unknown*, waarvan hij evenwel kan proberen het *risico* in te schatten. In het Web 2.0 zichtbaarheidsregiem van de informatiesamenleving is echter bij wijze van spreken de camera zelf onzichtbaar geworden. Er is hier sprake van een onzichtbare zichtbaarheid.[35] En indien men al een besef heeft van de mogelijkheid dat er zich achter het beeldscherm een database kan bevinden waarvan de verzamelde data worden onderworpen aan *datamining* en *profiling*, dan heerst er niet alleen onzekerheid over de vraag of dat in het onderhavige geval gebeurt, maar ook op welke wijze, en met welke doeleinden en door wie. Wie weet worden er wel, op een manier waarvan ik me geen enkele voorstelling kan maken, allerlei zaken over mij ontdekt, die ik zelf niet eens weet. Er is hier met andere woorden sprake van *unknown unknowns* en we ervaren geen risico, maar *onzekerheid*. In de eerste paragraaf merkte ik op dat de moderne, technologische samenleving door auteurs als Beck en Giddens wel wordt aangeduid als een risicosamenleving. De postmoderne informatiesamenleving is daarentegen primair een *onzekerheidssamenleving*.

Lessen voor de overheid

Welke lessen kan de Overheid 2.0 uit het voorgaande trekken? In de eerste plaats dat de overheid, wil zij het vertrouwen en de medewerking van burgers behouden of herwinnen, om te beginnen bij haar digitale dienstverlening een *vertrouwde digitale omgeving* dient te scheppen. Innovatie moet geen doel op zich zijn en steeds zal men bij vernieuwing het verlies aan vertrouwdheid moet verdisconteren. Vanuit dit perspectief kan *Slow Government* slechts worden toegejuicht! Ten behoeve van de vergroting van de gebruiksvriendelijkheid dienen de websites van de overheid bovendien *overzichtelijk* te zijn (waarbij zij nog veel van Google kan leren). Daarnaast dienen ze ook *transparant* te zijn en de gebruikers in klip en klare taal vertellen wat zich achter de beeldschermen afspeelt (op dit punt kan Google, die haar algoritmen angstvallig geheim houdt, dus allerminst als rolmodel dienen).[36] Zoals fabrikanten

van voedingsmiddelen en medicijnen verplicht zijn informatie te verschaffen over de aard en herkomst van de gebruikte ingrediënten, de bereidingswijze, contra-indicaties, mogelijke bijwerkingen etc., zo mag van de overheid worden gevraagd haar digitale dienstverlening vergezeld te laten gaan van 'digitale productinformatie' (welke gegevens worden gebruikt, waaraan worden zij gekoppeld, wat mag van het product worden verwacht en op welke termijn). Daarbij is ook de *contextuele integriteit* van groot belang.[37] Zoals de huisarts de vertrouwelijke medische gegevens van zijn patiënten in het kader van de behandeling wel mag delen met een medisch specialist, maar we niet graag zouden zien dat hij ze verkoopt aan een verzekeraar of een farmaceutische producent, zo dient de overheid zich in het geval zij de door de burger verschafte data aan andere data wil koppelen of met andere overheden wil delen steeds moeten afvragen of dit binnen de context van de onderhavige dienstverlening gerechtvaardigd is.

Met vertrouwdheid, transparantie en contextuele integriteit is de kous niet af. De mondige onlife burger wil niet alleen *inzicht* in zijn data, maar eist, zoals eerder opgemerkt, als actieve prod*user* van die data ook steeds vaker het *beheer* over die data op. Om als co-creator van de overheid te kunnen optreden is dat ook nodig. Dat gaat verder dan het door de Nationale ombudsman bepleitte recht om foutieve data te corrigeren.[38] We kunnen bijvoorbeeld denken aan de 'digitale burgerwacht', zoals die in 2014 in Barneveld zijn primeur beleefde.[39] Met deze *Cilivant*-groepsapp op de mobiele smartphone worden wijkbewoners met elkaar verbonden. Ze kunnen nu zelf melding maken van bijvoorbeeld een gestolen fiets of inbraak. Ook kunnen ze berichten over verdachte activiteiten rondom in te stellen 'volglocaties' ontvangen. Ze staan ook in verbinding met allerlei hulpdiensten, waarbij er sprake is van tweerichtingsverkeer. Met apps als deze wordt het persoonlijke vertrouwen dat in het verleden de cohesie van de kleine gemeenschap ondersteunde, op een gemedieerde wijze weer hersteld. Het Panopticum wordt hier als het ware gedemocratiseerd en omgevormd tot een "participerend panopticum."[40] De *digitale* dienstverlening van de overheid is daarbij eerder dan op het primaire proces (de fietsdiefstal, de inbraak) gericht op het bewaken van de kwaliteit en veiligheid van de benodigde informationele infrastructuur. Je zou dat kunnen vergelijken met een game designer, die niet zozeer zelf computerspellen speelt, maar daarentegen de database ontwerpt waarbinnen de spelers hun spel kunnen spelen.

Van de zijde van de overheid wordt op burgerinitiatieven als die in Barneveld vaak nogal aarzelend gereageerd. Dat heeft enerzijds te maken met de vrees voor de vervuiling van de data, die zou kunnen ontstaan wanneer burgers bijvoorbeeld zelf verantwoordelijk zouden worden voor hun gegevens in de Basisregistratie Personen (BRP), en anderzijds met de angst dat met die co-creatie de deur wordt opengezet voor misbruik. In de wereld van de Big Data is die vrees voor vervuiling de minste van de twee kwaden. Anders dan klassieke database managementsystemen, kunnen *datamining* en *profiling* prima uit de voeten met *messy data*, doordat de onvolledigheid of slordige codering – althans op macroniveau[41] – wordt gecompenseerd door het grote aantal.[42]

Misbruik door de burger is inderdaad een reëel risico. De grondhouding van de overheid naar de burger toe dient er een van vertrouwen te zijn, maar daarbij dient men te erkennen dat vertrouwen altijd gepaard gaat met onzekerheid over de verhoopte uitkomst. Het

werken met risicoprofielen kan de onzekerheid tot op zekere hoogte beheersbaar maken, maar nooit volledige garanties bieden. Datzelfde geldt overigens ook voor de burger, die immers (net als de consument) nooit volledig zeker kan weten of de beloofde transparantie en contextuele integriteit optimaal is en de beheerder van de databases volledig te vertrouwen. Het is niet ondenkbaar dat de Overheid 2.0 in digitale achterkamertjes stiekem toch allerlei geheime algoritmen loslaat op de data van de burgers. En door het mondiale karakter van het internet kunnen die achterkamertjes zich ook ver buiten de landsgrenzen bevinden.[43] Zelfs een uitgebreid systeem van *checks and balances* kan deze onzekerheid nooit volledig wegnemen.

Trouw

Toch is zowel voor de burger als voor de overheid van belang zich niet op te stellen als een jaloerse, wantrouwige minnaar die op een ziekelijke wijze alle gangen van de geliefde nagaat. Tot het tegendeel blijkt, dienen burger en overheid ervan uit te gaan dat de ander te goeder trouw is. Dat valt niet altijd mee. De overheid, beducht voor de sensatiezucht van de oude en nieuwe media, schiet nogal eens in de reflex haar trouw aan de burger te verruilen voor instrumenten die beloven zekerheid over de toekomst te garanderen. Een dergelijk geloof, dat vaak ten grondslag ligt aan de megalomane ICT-projecten van de overheid, ontkent de toevalligheid van het leven. Met als gevolg dat die projecten vaak tegen beter weten in worden doorgezet in het aangezicht van hun mislukking.

In het tijdvak van de Big Data neemt het geloof in de mogelijkheid van de eliminatie van het toeval zelfs een voor het vertrouwen bijzonder gevaarlijke wending. Zoals ik hierboven opmerkte, is het met behulp van *datamining* mogelijk voorspellingen over de toekomst te doen. Als deze techniek wordt gebruikt om de boekliefhebber op de hoogte te stellen welk boek hij volgende week zal willen gaan lezen, of om de verspreiding van een griepvirus te voorspellen, dan lijkt daar nog niet zoveel tegen te zijn; het is dan zelfs een nuttig instrument. Het wordt al anders wanneer men het Digitaal Kinddossier gaat aanwenden om preventief in te grijpen in de opvoedingssituatie. Zeker wanneer men dan onwillekeurig moet denken aan de film *Minority Report* (2002) van Steven Spielberg, waarin wordt verhaald van een toekomstige wereld waarin potentiële moordenaars op basis van onfeilbaar geachte voorspellingen preventief worden opgesloten. Natuurlijk willen we voorkomen dat kinderen worden verwaarloosd of mishandeld en dat wordt verhinderd dat moordenaars hun slag kunnen slaan, maar het is de vraag of hier het middel niet erger is dan de kwaal.

Voorspellingen die zijn gebaseerd op *datamining* en *profiling* zijn gebaseerd op het vinden van correlaties. “Knowing *what*, not *why*, is good enough”.[44] Binnen de context van de overheid impliceert dit, dat louter het optreden van specifieke correlatie ingrijpen in het leven van de burger rechtvaardigt. Wie een enkeltje New York met een halal maaltijd reserveert, maakt ongeacht zijn of haar bedoelingen weinig kans zonder problemen het vliegtuig in te stappen. Het taalspel van *agency* en handelingscausaliteit, volgens welke mensen handelen op basis van intenties, motieven en redenen, maar daarvan soms ook afwijken (dat is inherent aan menselijke vrijheid), wordt hier buiten spel gezet. Chaotische systemen zoals de menselijke samenleving zijn echter nooit volledig voorspelbaar. Wie meent dat dit wel het geval is en op basis van louter correlaties hoopt zekerheid te verkrijgen, loopt het gevaar een zelfvervullende

profetie te begaan. Daarmee is niets minder dan de menselijkheid van de mens in het geding.[45]

Een menswaardig bestaan veronderstelt naast vertrouwdheid en vertrouwen ook het in gelegenheid worden gesteld *trouw* te blijven aan zichzelf. Wanneer we een boek lenen van een vriend, dan is het teruggeven daarvan geen feitelijk gegeven, maar de morele opgave die belofte gestand te doen. Gesteld dat het mogelijk zou zijn door een perfecte technologie de mogelijkheid te elimineren een geleend boek niet terug te geven, dan zou er wellicht toe leiden dat er minder boeken voorgoed uit onze boekenkasten verdwijnen, maar het zou ook datgene elimineren dat vriendschap zo waardevol maakt in het leven.

Misschien wel de belangrijkste les voor de digitale overheid

Wanneer we willen dat de overheid trouw blijft aan haar burgers en de burger trouw aan de overheid, dan eist dat dat zij zichzelf en elkaar *vertrouwen*. En dat vereist op zijn beurt een *fundamentele bereidheid tot onzekerheid*. Die biedt weliswaar geen garantie op eeuwigdurende veiligheid en vrede, maar stelt ons wel in staat een leefbare balans te behouden tussen de menselijke behoefte aan veiligheid en de niet minder fundamentele vrijheidsdrang. En zij voorkomt dat de barbaarse natuurtoestand waarvan Hobbes spreekt, zich al te vaak opnieuw voltrekt.

Eindnoten

Bij het schrijven van deze tekst conform de opdracht gekozen voor een essayistisch, dat wil zeggen een explorerend en enigszins speels betoog. Dat neemt niet weg dat ik rijkelijk heb geput uit uiteenlopende wetenschappelijke en filosofische bronnen en uit eerdere, meer systematische studies. De belangrijkste daarvan worden in de eindnoten genoemd. Ik dank Frank Faber, Esther Keymolen, Elize de Mul, Awee Prins en Vivian Visser voor hun commentaar op een eerdere versie van deze tekst. Het onderzoek dat mijn promovenda Esther Keymolen (inmiddels werkzaam bij eLaw, het Centrum voor Recht en Digitale Technologie van de Rechtenfaculteit van Universiteit Leiden) doet naar de impact van het internet op vertrouwensrelaties vormde een belangrijke inspiratiebron voor de paragraaf 'Velerlei vertrouwen' .

[1] De burger gaat digitaal. Onderzoeksrapport Nationale Ombudsman nr. 2013/170. https://www.nationaleombudsman.nl/uploads/2013170_de_burger_gaat_digitaal.pdf, blz. ii-iii.
[2] Thomas Hobbes, *Leviathan.* Harmondsworth: Pelican, 1976 blz.186.
[3] Zie Marshall David Sahlins, *Stone Age Economics*. Chicago: Aldine-Atherton, 1972.
[4] Jos de Mul, *Destiny Domesticated. The Rebirth of Tragedy Out of the Spirit of Technology.* Albany: State University of New York Press, 2014.
[5] Niklas Luhmann. *Trust and Power. Two works by Niklas Luhmann.* New York: John Wiley & sons Ltd, 1979.
[6] Anthony Giddens, *The consequences of modernity*. Cambridge, UK: Polity Press in association with Basil Blackwell, Oxford, UK, 1990, 83.
[7] Anthony Giddens, *The consequences of modernity,* a.w., en Ulrich Beck, *Risikogesellschaft : Auf dem Weg in eine andere Moderne.* Frankfurt am Main: Suhrkamp, 1986.
[8] Esther Keymolen. *Trust on the line. A philosophical Perspective on the Experience of Trust through Internet Technology* (proefschrift in wording), hoofdstuk 3.
[9] Alvin Toffler, *The Third Wave*. New York: Morrow, 1980.
[10] Manual Castells. *The Information Age: Economy, Society and Culture.* 3 Volumes. Oxford: Blackwell Publishers, 1996-97.

[11] Jos de Mul, The Informatization of the Worldview. *Information, Communication & Society* Vol. 2, no. 1 (1999): 604-29.

[12] Luciano Floridi, (ed.)., *The Onlife Manifesto. Being Human in a Hyperconnected Era*. Heidelberg/ New York/Dordrecht/ London: Springer, 2015.

[13] Viktor Mayer-Schönberger and Kenneth Cukier, *Big Data. A Revolution That Will Transform How We Live, Work, and Think*. Boston: Houghton Mifflin Harcourt, 2013.

[14] Max Welling, *Van veel data, snelle computers en complexe modellen tot lerende machines*, Oratie Universiteit van Amsterdam, 2014.

[15] Zie het hoofdstuk "Neurotica: het zwermgeest scenario" in Jos de Mul, *Kunstmatig van nature. Onderweg naar Homo sapiens 3.0*. Rotterdam: Lemniscaat, 2014, blz. 101-130.

[16] Natasha Lomas, Amazon Patents "Anticipatory" Shipping – To Start Sending Stuff Before You've Bought It, http://techcrunch.com/2014/01/18/amazon-pre-ships/, geraadpleegd op 2 juni 2015.

[17] Mayer-Schönberger and Cukier, a.w.

[18] Zie WRR, *De publieke kern van het internet. Naar een buitenlands internet beleid*. Den Haag: WRR, 2015.

[19] Een overtuigende literaire verbeelding daarvan biedt het korte verhaal 'De bibliotheek van Babel' van de Argentijnse auteur Jorge Luis Borges, dat handelt over een bibliotheek die bestaat uit een verzameling boeken, die ieder 410 bladzijden bevatten, die op hun beurt ieder 40 regels van 80 lettertekens tellen (zie http://hyperdiscordia.crywalt.com/library_of_babel.html). Het bijzonder van de bibliotheek is, dat iedere mogelijke combinatie van de 25 tekens van het Spaanse alfabet (22 letters, aangevuld met de punt, komma en spatie) in één van de boeken is gerealiseerd. Dat wil zeggen dat de bibliotheek $25^{1.312.000}$ (d.w.z. 25 letters tot de macht 410 x 40 x 80) boeken bevat, ofwel in meer gebruikelijke machten van 10 geschreven ca. $10^{1.834.097}$ boeken. Als we bedenken dat Google ongeveer een biljoen (10^{12}) webpagina's heeft geïndexeerd en dat het universum volgens schattingen van astrofysici ca.10^{80} atomen bevat, dan beginnen we te beseffen wat een hyperastronomische hoeveelheid combinaties er van slechts 25 tekens mogelijk zijn. Zelfs wanneer ieder atoom in het universum een boek uit de Bibliotheek van Babel zou kunnen bevatten, zou de hoeveelheid boeken in ons universum verwaarloosbaar klein zijn in vergelijking met de door Borges verbeelde bibliotheek. 'De bibliotheek van Babel' zou verplichte kost moeten zijn voor iedere ambtenaar die te maken heeft met *datamining* en *profiling*. Op het internet kan men diverse websites vinden waar men boeken uit de bibliotheek van Babel kan genereren. Zie bijvoorbeeld http://libraryofbabel.info/index.html.

[20] De Mul, *Destiny Domesticated. The Rebirth of Tragedy Out of the Spirit of Technology*. a.w., blz. 7v.

[21] Algemene Rekenkamer. *Lessen uit ICT-Projecten bij de overheid*. Den Haag, 2008, blz.1. Ik moet nog vaak denken aan de profetische woorden die Johan van Wamelen, destijds directeur Informatiemanagement en Organisatie van het Ministerie VROM en samen met Paul Frissen en mijzelf initiator van de denktank Internet & Openbaar Bestuur, ons in 1998 voorhield over informatiseringprojecten bij de overheid: "Wanneer je standaard ervan uitgaat dat het tweemaal zo lang duurt en viermaal zoveel kost dan begroot, dan valt het soms niet tegen".

[22] http://www.nrc.nl/nieuws/2014/06/21/geflopt-ICT-project-kostte-belastingdienst-ruim-200-miljoen-euro/

[23] http://www.binnenlandsbestuur.nl/digitaal/nieuws/duurste-ICT-project-van-de-overheid-gestopt.9473221.lynkx

[24] Algemene Rekenkamer. *Lessen uit ICT-projecten bij de overheid*. Den Haag, 2008, blz.1.

[25] Raad voor het Openbaar Bestuur en Raad voor Cultuur. *Informatie: Grondstof met toekomstwaarde. Contouren Van een visie op de rol en betekenis van informatie*. Den Haag, 2008. Dat deze kritiek niet geheel aan dovemansoren is gericht bewijst de Taskforce Bestuur en Informatieveiligheid Dienstverlening (Taskforce BID), die mede op advies van de Onderzoeksraad voor Veiligheid op 13 februari 2013 door minister Plasterk (BZK) voor een periode van twee jaar in het leven is geroepen. Zie www.taskforcebid.nl.

[26] Jos de Mul, De kunstmatig intelligente overheid, in *Jaarcongres De intelligente overheid*. Rotterdam: Center for Public Innovation, 2009, blz. 39-44.

[27] Victor Bekkers en Ron Foederer (red.) *De belastingdienst: ICT, afstand en compliance*. In: Stavros Zouridis, Paul Frissen, Nicole Kroon, Jos de Mul en Johan van Wamelen (red.) *Internet en Openbaar Bestuur II*, Den Haag: Onderzoeksprogramma Internet en Openbaar Bestuur, 2001.

[28] Valerie Frissen, *Big Society, Big Data. The Radicalisation of the Network Society*. The Hague: The Hague

Center for Strategic Studies/TNO, 2011.

[29] Zie http://www.ambtenaar20.nl/

[30] Jeron Lanier, *Who Owns the Future?*, Simon & Schuster, New York, 2013.

[31] Zie in dit verband ook Mireille Hildebrandt, ICT en rechtsstaat, in S. van der Hof, A.R. Lodder en G.J. Zwenne (red.), *Recht en computer*. Deventer: Kluwer, 2014, 25-45.

[32] http://recruitmentmatters.nl/2013/11/09/waarom-werk-nl-niet-goed-werkt/

[33] Esther Keymolen, Trust and technology in collaborative consumption. Why it is not just about you and me. In R. Leenes, & E. Kosta (Eds.), *Bridging Distances in Technology and Regulation*. Tilburg: Wolf Legal Publishers, 2013, blz. 135-150.

[34] Michel Foucault, M. *Surveiller et punir. Naissance de la prison.* Paris: Gallimard, 1975.

[35] Esther Keymolen, *Onzichtbare Zichtbaarheid. Helmuth Plessner Ontmoet Profiling*, BA thesis. Erasmus University, 2007. Zie ook Mireille Hildebrandt, Who is profiling who? Invisible visibility. In S. Gutwirth, Y. Poullet, P. Hert, C. Terwagne & S. Nouwt (eds.). *Reinventing Data Protection?*, Rotterdam: Springer Netherlands, 2007.

[36] Dit is ook een van de adviezen van de Nationale ombudsman in het eerder genoemde onderzoeksrapport *De burger gaat digitaal*, a.w., blz. 23, 47. Vanzelfsprekend zijn er grenzen aan deze transparantie. Bepaalde veiligheidstaken vereisen geheimhouding. Maar zelfs dan kan in de meeste gevallen van de overheid worden gevraagd duidelijkheid te verschaffen over in welke gevallen welke data voor welke doeleinden kunnen worden gebruikt.

[37] Zie Helen Nissenbaum, Privacy as contextual integrity. *Washington Law Review* 79(1), 2004, 119-157.

[38] Idem, a.w. blz. 37 **.**

[39] http://www.emerce.nl/wire/barneveld-heeft-eerste-digitale-burgerwacht-nederland

[40] James Cascio, The Rise of the Participatory Panopticon, 2005. http://www. worldchanging.com/archives/002651.html.

[41] Voor de overheid die big data analyse gebruikt, zijn vervuilde data geen probleem. Die kleine foutmarge is te verwaarlozen als de output maar hoog blijft. Voor de burger is het momenteel een drama wanneer hij de pech heeft om in die foutmarge te belanden. De ombudsman heeft schrijnende gevallen gedocumenteerd van personen die foutief in databases staan en daar ontzettend veel last van ondervinden en op één of andere manier heel moeilijk uit al die verknoopte databases te zetten zijn. Door de burger de regie over zijn persoonsgegevens te geven, wordt hij in staat gesteld door de overheden of hemzelf gemaakte fouten zelf te herstellen.

[42] Zie de hoofdstukken “More” en “Messy” in Mayer-Schönberger en Cukier, a.w.

[43] Zie noot 18. Een recent voorbeeld is de door het Oostenrijkse parlementslid Peter Pilz tijdens een persconferentie in Brussel onthulde aftappen sinds 2005 van tientallen internetverbindingen tussen Nederland en het buitenland door de Duitse inlichtingendienst BND en de Amerikaanse NSA. http://www.nrc.nl/nieuws/2015/05/28/ parlementarier-levert-bewijs-voor-duitse-spionage-in-nederland/

[44] Mayer-Schönberger and Cukier, a.w., blz. 52.

[45] Jos de Mul, Database Identity: Personal and Cultural Identity in the Age of Global Datafication. in: Wouter de Been, Payal Aurora and Mireille Hildebrandt (Eds.), *Crossroads in New Media, Identity and Law. The Shape of Diversity to Come. Personal and Cultural Identity in the Age of Global Datafication*. Basingstoke/New York: Palgrave Macmillan, 2015, 97-118.