Essay ethiek in de digitale samenleving
erica pierik

Vrije wil, onbewuste wil of gestuurd gedrag in de digitale samenleving

Inleiding

Technologische ontwikkelingen gaan razendsnel – sneller dan wij als mensen bij kunnen houden. Het internet is alomtegenwoordig, maar steeds vaker op de achtergrond. Er spelen daarmee twee verschillende zaken een rol: wij begrijpen lang niet alles van de techniek waar we evengoed wel gebruik van maken, en die techniek is niet langer zichtbaar en merkbaar. De vraag of wij zelf verantwoordelijk kunnen worden gehouden voor onze acties op digitaal gebied, wordt daarmee steeds minder eenduidig te beantwoorden.

Dit essay gaat in op vragen die vanuit gebruikers gesteld kunnen (moeten?) worden. Waar lopen we als gebruiker in de digitale wereld tegen aan? Aan de hand van alledaagse persoonlijke voorbeelden ga ik dieper in op de ethische kwesties die ten grondslag liggen aan de verantwoordelijkheidsvraag. Ik geef geen antwoorden, want die heb ik ook niet. Daarbij zijn er meerdere werkelijkheden en heeft een mogelijke oplossing ook vaak nadelen. Veel van waar we nu mee te maken hebben kent geen precedent: nooit eerder leefden we in een wereld met zo veel informatie, data en digitale mogelijkheden.

Ik begin met een korte inleiding over privacy in onze digitale maatschappij – hoe er steeds meer mogelijk is zonder dat we nog kunnen begrijpen waarom, en hoe mensen daar gebruik (of misbruik) van kunnen maken. De daar bij komende onzichtbaarheid van deze techniek maakt dat we (vaak onbewust) gestuurd worden in bepaalde gedragingen of reacties. Het tweede deel richt zich op de grenzen van privacy en dataverzameling: zijn die grenzen er en wie houdt ze in de gaten? Het derde deel gaat in op veiligheid in een digitale samenleving: wie beschermt ons, als zelfs de overheid het niet allemaal in de hand heeft? Ik eindig met de vraag of er behoefte is aan nieuw beleid, en wie dat vorm gaat geven.

De grenzen tussen privacy en dataverzamelingen en veiligheid zijn lang niet altijd scherp, overlappen elkaar soms en spreken elkaar tegen. Ook de overwegingen om wel of niet privacy te respecteren, wel of niet dataverzamelingen aan te leggen en vanuit welk oogmerk (commercieel, innovatie, kostenbesparing) en wel of niet overheidsingrijpen te willen zijn niet eenduidig te bezien. De twee belangrijkste vragen zijn steeds: wat willen we en wie is verantwoordelijk?

Privacy in de digitale wereld

In 2013 werden de risico's van privacy schending al onderkend door de overheid. In een visie op e-privacy van 24 mei geven ze onder andere het volgende aan:

> "Veel Nederlanders maken gebruik van innovatieve, online toepassingen. Deze toepassingen bieden de eindgebruiker vaak gratis, handige diensten. Het gebruik van deze diensten gaat gepaard met het vrijgeven van persoonsgegevens, waarvan bedrijven gebruik maken. Deze persoonsgegevens zijn voor bedrijven interessant en geld waard. Persoonsgegevens vertegenwoordigen dus in toenemende mate een belangrijke economische waarde. Door deze

persoonsgegevens af te geven kunnen handige diensten afgenomen worden, maar ontstaat ook een privacyrisico."

"De eindgebruiker lijkt weinig grip te hebben op de ontwikkelingen op het terrein van de gegevensverwerking en het gebruik ervan. De gebruikers zijn zich niet altijd bewust, of op de hoogte van wat derden met hun persoonsgegevens doen, en welke impact dat heeft in de online wereld. Tegelijkertijd moeten consumenten akkoord gaan met privacyvoorwaarden om gebruik te kunnen maken van bepaalde diensten, of voor het kunnen kopen van producten. De teksten van de voorwaarden zijn veelal lang, complex en gezien het juridische jargon niet voldoende te begrijpen voor een gemiddelde eindgebruiker."

"Een vinkje bij de privacyvoorwaarden ontslaat een organisatie er niet van de privacy van hun klanten te respecteren en hiertoe helder te communiceren over waarom en hoe organisaties en derde partijen met persoonsgegevens en persoonlijke data van hun klanten omgaan."

Toch legt de overheid een flink deel van de verantwoordelijkheid bij de gebruikers, die – in hun woorden – "bewust of onbewust persoonlijke gegevens achterlaten op het web. Hierdoor neemt het risico op verlies en misbruik van persoonsgegevens (identiteitsfraude) toe." Wel zien zij een rol voor zichzelf in het samen overleggen met de leveranciers van hardware en software over hoe zij ICT-systemen veiliger kunnen maken.

Op dit moment liggen er twee concept wetsvoorstellen bij de Tweede Kamer: de Wet inlichtingen- en veiligheidsdiensten (Wiv) en Wet computercriminaliteit III. Deze beide wetten breiden de bevoegdheden van geheime diensten en politie op het web aanzienlijk uit. In consultatierondes hebben bedrijfsleven en ICT-instellingen aangegeven dat deze wetten zelfs uit oogpunt van veiligheid te ver gaan. Mag een overheid van een maatschappij verwachten dat particulieren en bedrijfsleven de wetten van e-privacy naleven, en tegelijkertijd vanuit het idee van veiligheid rijksdiensten veel vrijheid geven in het opsporen van misbruik?

<u>Vrije wil, onbewuste wil of gestuurd gedrag</u>
Als ik inlog op Facebook, krijg ik een pop up op mijn scherm: de voorwaarden zijn weer eens veranderd en of ik daar mee akkoord ga. Ik zucht en scroll snel naar beneden om op "I agree" te klikken. Gezeur.

Sinds 1 januari 2014 heeft Facebook in de voorwaarden opgenomen dat het bedrijf het surfgedrag van gebruikers ook op andere websites mag volgen. Sinds begin 2015 mogen ook de profielfoto en bijhorende naam opgenomen worden in advertenties. Deze gegevens zijn razend interessant voor (betalende) adverteerders. Gebruikers kunnen hier niet zo heel veel tegen doen: je accepteert het doorspelen van jouw gegevens (data) of je stopt met Facebook. Er worden, op grond van de privacywet weliswaar geen directe overtredingen begaan, toch begeeft Facebook zich met deze praktijken op een grijs gebied. De privacywet stamt immers uit een tijd waarin Facebook -en bijhorende privacyvraagstukken- nog niet bestonden.

Deze praktijken leiden tot gerichtere advertenties op Facebook, die passen bij de wensen en behoeften van de gebruiker. Als iemand op zo'n advertentie klikt ("Kijk nou! Da's toevallig!") is dat dan vrije wil of gestuurd gedrag? Betreft dit beïnvloeding van keuzes door een van tevoren aangeboden prikkel die niet bewust wordt waargenomen? De gebruiker had er immers ook niet op kunnen klikken, maar Facebook heeft geconstateerd dat hij of zij daar behoefte aan had, dus…

Hoe wenselijk of ethisch is dit? Is het meedenken, besluiten uit handen nemen en je leven laten vergemakkelijken door (online) technologie? Of is het kapitalistische “nudging” waar we als vrijdenkende wezens tegen in opstand zouden moeten komen?

Is het bovenstaande een vorm van oneigenlijk gebruik van data? Wie is verantwoordelijk voor dergelijke acties van Facebook? De gebruiker die niet alleen de voorwaarden heeft geaccepteerd, maar ook zelf een bepaalde post heeft geplaatst? Facebook, omdat het rechtmatig verkregen informatie oneigenlijk gebruikt? Of de overheid, die dit soort misbruik hoort te voorkomen? En willen we dat?

Privacy en Big Data

De ondoorzichtigheid van dataverzameling

Omdat ons internet hapert, bel ik met de klantenservice van Ziggo. Ik luister geduldig naar het “in de wacht”-muziekje tot er verbinding komt met een medewerker. Nog voor ik mijn mond open doe zegt de medewerker aan de andere kant van de lijn vrolijk: “Goedemorgen mevrouw Pierik, waarmee kan ik u helpen?” Na de eerste verbazing geeft hij op verzoek aan dat mijn telefoonnummer van de mobiel waar ik mee bel, gekoppeld is aan mijn klantgegevens. Zonder dat ik maar iets hoef te doen, ziet hij direct waar ik woon, welk pakket wij hebben en zelfs hoe de internetverbinding de afgelopen maanden gefunctioneerd heeft.

Handig of ontoelaatbaar? In het bovenstaande geval is de koppeling van data aan een persoon gedaan zonder expliciete toestemming. ING deed iets vergelijkbaars in 2014, door aan te kondigen klantgegevens met toestemming te willen verkopen aan adverteerders, dat door de vele protesten uiteindelijk niet doorging. Begin 2015 echter kondigde Achmea aan de klanten om data en gegevens te vragen in ruil voor korting op de verzekeringen. Privacygegevens worden hierdoor een valuta: betalen met je persoonlijke gegevens.

Veel data worden verzameld door grote technologiebedrijven. Microsoft, Apple, Google en Facebook zijn precies op de hoogte van ieders internetgedrag. Al die data zijn echter niet alleen bij hen bekend, maar worden tevens massaal verzameld door overheden. Het aanleggen van big data verzamelingen is voor sommigen juist een voorwaarde voor innovatie. Uit alle verzamelde data wordt met een analyse gekeken naar behoefte aan nieuwe diensten of toepassingen – een behoefte die zonder big data niet naar voren zal komen. Het verzamelen en analyseren van big data geeft nieuw inzicht in de voorkeuren en het gedrag van gebruikers op, en leidt daarmee tot nieuwe innovaties.

Wat weegt dan zwaarder; dataverzameling voor innovatie, of strikte privacy bescherming? Is dit wel af te wegen? Is er een middenweg? En wie bepaalt deze dan? Bovendien is deze afweging voor iedereen anders: sommigen zullen het gemak voorop stellen, anderen hechten meer waarde aan de privacy. Is dit individueel op te stellen? Kunnen we toe naar een systeem waarbij we per website, transactie of vraag aangeven in hoeverre we toestemming voor dataverzameling geven? Geen dichtgetimmerde voorwaarden van dertig kantjes, geen voortdurend pop-up scherm zoals met de cookies, maar gewoon voordat we op “send” klikken een vraag wat we met onze gegevens willen?

Grenzen van privacy

De introductie van de OV-chipkaart in 2010 leidde al na enkele weken tot de eerste succesvolle pogingen deze te hacken. Drie jaar lang werd gewerkt aan betere beveiliging, maar in 2013 was een nieuwe hack al weer een feit. Ook de nog betere beveiliging in 2015 was een kort leven beschoren; het hacken van de OV-chipkaart werd gezien als een nationale sport en uitdaging.

Privacy is een ingewikkeld begrip met meerdere betekenissen. Enerzijds verwijst privacy naar het persoonlijke, het niet voor publiek zichtbare, anderzijds op dat wat een persoon tot uniek individu maakt. Recente ontwikkelingen hebben de definitie van privacy uitgebreid met “niets te verbergen”, zodat overheden zich grotere vrijheden konden permitteren om vanuit oogpunt van veiligheid de grenzen van privacy op te rekken. Niet alleen om te screenen, maar ook om deze gegevens op te slaan voor eventueel later gebruik.

De elektronische gegevens bij de overheid moeten goed beveiligd zijn. Vaak gaat het om gevoelige informatie die de mensen waar het om gaat kwetsbaar maakt als deze publiek wordt. Zo is begin 2015 gebleken dat het systeem dat gemeenten gebruiken om te onderzoeken of mensen recht hebben op een uitkering lek is. Niet alleen hadden andere dan de rechtmatige ambtenaren toegang tot deze gegevens, ook commerciële incassobureaus konden het systeem gebruiken. Dat schaadt het vertrouwen dat mensen in de overheid, maar ook in de veiligheid van digitale systemen hebben.

Het is ondertussen duidelijk dat steeds meer data en gegevens opgeslagen worden. Sommige gegevens vrijwillig en bewust, zoals alles wat je als gebruiker zelf op internet zet, sommige gegevens vrijwillig en onbewust. Wie een uitkering aanvraagt, verstrekt vrijwillig gegevens aan de overheid, maar de opslag en beveiliging daarvan heeft de aanvrager niet zelf in de hand. In onze maatschappij is een niveau van surveillance gaande waar we nog niet eerder mee te maken hebben gehad. Iedereen laat bewust en onbewust digitale sporen na, via internet, z’n mobiele telefoon of via dataopslag in systemen.

Al deze sporen worden gemonitord, dus ook die we onbewust achterlaten. Het internationale recht is onvoldoende ingericht op deze massale gegevensverzamelingen en transnationale surveillance. Waar liggen de grenzen van dataverzameling? Als we zelf niet langer verantwoordelijk zijn voor gegevensverstrekking, wie is dan verantwoordelijk voor de privacy waarborging hiervan?

Een veilige samenleving

De Digitale Overheid
Mijn schoonouders van in de 80 zijn verhuisd naar een seniorenappartement en hebben hun gezinswoning te koop gezet. De makelaar wijst ons op het feit dat het verplicht is om een energielabel aan te vragen bij verkoop. We gaan op zoek naar de website en kom er al snel achter dat een energielabel alleen met DigiD aan te vragen is. Mijn bejaarde schoonouders hebben geen email en geen mobiele telefoon, dus het aanvragen van een DigiD is onmogelijk, en daarmee het aanvragen van een energielabel ook, terwijl dat wel verplicht is. Wat nu? Frauderen en op naam van mijn schoonouders een DigiD aanvragen?

Een digitale overheid heeft grote voordelen. Het scheelt papier, is sneller en goedkoper, zowel in porto als in doorlooptijden. Voor ouderen, slechtzienden en digibeten is het echter niet zo gemakkelijk. Toch denkt de overheid dat ook zij met voldoende ondersteuning digitaal kunnen worden. Die ondersteuning bereikt op dit moment nog niet alle ouderen, en het is de vraag of dat kan. Anno 2017 is de burger er zelf verantwoordelijk voor zijn om zijn of haar digitale zaken op orde te hebben, en zal papier steeds meer verdwijnen. Belastingen, wijzigingen, aanvragen zullen allemaal digitaal moeten, wat mensen met een digitale achterstand in een kwetsbare positie brengt. Dit dilemma van efficiency ten opzichte van inclusiviteit en de menselijke maat, is de kern van de vraag *voor wie doe je het?*

Ook nu al is het zo dat wijzigingen digitaal doorgegeven moeten worden, en dat wie kiest voor een telefonisch doorgegeven wijziging, daar een onevenredig hoog bedrag voor neer moet tellen, terwijl online wijzigen gratis is. Die ongelijkheid wordt alleen maar groter en

vergroot tevens de kans op de hierboven genoemde fraude – vanuit frustratie. De keuze om voor volledig digitaal te gaan, sluit niet uit om de reguliere kanalen beschikbaar te houden voor wie daar voor kiest.

DigiD is bovendien fraudegevoelig. Een inlogsysteem met alleen een inlognaam en een wachtwoord (eventueel met extra controle via sms) is niet langer veilig en bruikbaar. DigiD blijkt gemakkelijk te kraken, waarbij vreemden toeslagen kunnen aanvragen op een ander rekeningnummer. Bij constatering van onrechtmatig gebruik van toeslagen, wordt het teveel uitgekeerde verhaald op de eigenaar van de DigiD en wordt het onterecht uitgekeerde bedrag teruggevorderd. Het is vervolgens aan de eigenaar van de DigiD om te bewijzen dat er gefraudeerd is - wat bijna niet te corrigeren is, zelfs als de benodigde informatie bij de overheid aanwezig is.

In augustus 2013 was er een grootschalige Ddos aanval op DigiD, wat leidde tot een verplichte aanscherping van de eisen van het DigiD-wachtwoord bij de Belastingdienst, en een extra controle per sms. Ook wordt er al enige tijd gewerkt aan een nieuw en hackproof systeem dat Idensys gaat heten. Hoe dat er uit komt te zien is nog niet bekend.

Is het de oplossing om alle digitale overheidsdiensten te voorzien van steeds nieuwere beveiligingsmethoden? Of misschien om het inzien van persoonlijke gegevens te beperken? Of een extra controle in te voeren bij het aanvragen van toeslagen, om fraude te voorkomen? Is het steeds verder dichttimmeren van digitale voorzieningen noodzaak of een extra beperking? Zijn er nog andere manieren om persoonlijke gegevens te beveiligen?

Veiligheid

Omdat mijn paspoort verlopen is, begeef ik mij opgewekt naar het stadhuis om een nieuwe aan te vragen. Ik heb alles bij me; het oude paspoort, chagrijnige pasfoto's en mijn betaalpas. Als ik aan de beurt ben, moet ik tot mijn grote verbazing een vingerscan laten maken. Dat wil ik niet – ik ben een onschuldige burger en geen crimineel! Waar is dat goed voor?! Maar weigeren heeft geen zin – of een vingerscan, of een leven zonder paspoort.

Een vingerscan voor een nieuw paspoort is verplicht sinds 2003. Dat staat in de Europese richtlijnen voor reisdocumenten, opgesteld door de EU na sterk aandringen van de VS. Rechtszaken over weigering hiervan door boze burgers belandden in 2012 bij de Raad van State en in 2013 bij het Europese Hof van Justitie. Deze oordeelden dat opslag en gebruik van vingerafdrukken in databanken niet onder de werking van de Europese Paspoortverordening valt en laat de toetsing van dergelijke opslag over aan nationale rechters en het Europees Hof voor de Rechten van de Mens in Straatsburg. Alle individuele rechtszaken hieromtrent zijn tot nog toe zonder succes.

Van de vingerafdrukken komen er twee op de chip in het biometrische paspoort, en vier worden opgeslagen in een speciale databank. Behalve goodwill van de VS zorgt deze opslag ook voor snellere opsporing bij criminaliteit en identiteitsfraude.

Is het verplicht afgeven van kenmerkende fysieke eigenschappen een inbreuk op je privacy? Wie is verantwoordelijk voor een correcte data-opslag? Wie zorgt ervoor dat onbevoegden geen toegang krijgen tot deze data en wie is er verantwoordelijk wanneer het misgaat?

Op Schiphol is sinds kort de Security Scan ingevoerd – een soort bodyscan met hetzelfde effect als fouilleren, zonder fysiek contact. De verschillen met de vingerafdruk op het paspoort zijn groot:

- de Security Scan mag geweigerd worden
- de beelden worden geanalyseerd door een computer en niet door een operator
- de data wordt alleen gebruikt voor de analyse en niet opgeslagen

Is dit een oplossing? Extra veiligheid voor wie dat wenst, inclusief sneller en effectiever resultaat? Geen mensen maar machines die analyseren? Geen opslag van de vingerscan, maar alleen als toets of paspoort en houder bij elkaar horen?

Ethische keuzes in het maken van nieuw beleid

Als gebruikers van digitale technologie nemen wij beslissingen en acteren daarnaar. Dat kan onbewust zijn, uit vrije wil of door externe factoren gestuurd. Niet alles wat we doen is dus bewust. Ik denk zelf dat er toch wel iets van een “wil” in mij huist; geen input - output maar input - proces – output. Iets in mij bepaalt mede mijn gedrag. Maar of dat nu vrije wil, het onbewuste of gestuurd is - alles is te beïnvloeden. De vraag is of we dat willen beperken, voorkomen of controleren.

De ethische keuzes die voortkomen uit de informatiesamenleving zijn volgens mij niet te reguleren door wetten vast te stellen en afspraken te maken. Dat beperkt innovatie en ontwikkeling, en houdt tegelijkertijd oneigenlijk gebruik van data niet tegen. Het onbewuste leven dat als een soort digitale laag om ons heen hangt, is misschien te vergelijken met het gat in de ozonlaag – je ziet het niet, maar het is er wel en het heeft consequenties. Door de steeds groeiende bewustwording van opwarming van de aarde, is er een nieuwe beweging ontstaan die denkt en acteert vanuit duurzaamheid.

Misschien is dat voor de digitale samenleving ook de beste benadering: zorg voor bewustwording en dan komt de samenleving op termijn met nieuw gedrag die de schadelijke consequenties zo veel mogelijk probeert te vermijden. Het zal een lang proces zijn, maar wel vanuit de burger -als *maker* van de digitale samenleving en niet als passieve gebruiker.