Terug naar de elektronische snelweg; gedachten over een data-APK en een datawacht.[1]

Liesbet van Zoonen

Laten we eens uitproberen wat er gebeurt als we over privacy nadenken met behulp van verkeersmetaforen. Tenslotte spraken we ooit over internet als ware het een 'elektronische snelweg'. Welnu, voor een snelweg heb je een vervoersmiddel nodig; een auto op de snelweg en je persoonlijke data op de elektronische snelweg, of dat nou gegevens zijn die van je afgenomen worden (cookies) of die je zelf overlegt (registraties). Die gegevens zijn als een auto: je wilt niet dat iemand ze steelt, je wilt dat ze het goed doen (correct zijn) en dat ze niet onbruikbaar worden (omdat je weer eens een paswoord vergeten bent). Dus net als een auto, moeten je gegevens op slot kunnen, moeten ze in goede staat zijn en moeten ze snel gerepareerd kunnen worden. Ik ga daarom in dit essay betogen dat we voor onze persoonlijke data, net als voor de auto, een jaarlijkse APK nodig hebben en een 'datawacht' die kan uitrukken als onmiddellijke reparatie nodig is. Om bij die eindbestemming van dit essay te komen, doe ik eerst de privacy paradox aan, dan stop ik bij de gedachte dat controle over data belangrijker is dan privacy, maar die gedachte leidt weer naar een nieuwe paradox. Daarom kies ik uiteindelijk de alternatieve route naar de data-APK en de datawacht.

Privacyparadox

Als je Nederlanders de open vraag stelt welk maatschappelijk probleem ze het liefste morgen opgelost zouden zien, dan zeggen ze ouderenzorg, werkloosheid, milieu, en in een paar gevallen Islam. Die agenda wordt anders als je mensen een lijst met problemen voorlegt en hen vraagt welke met voorrang aangepakt moeten worden. Op die lijsten komt tegenwoordig ' privacy' voor en dat scoort als probleemgebied steeds hoger. De politieke barometer van IPSOS laat bijvoorbeeld zien dat het aantal mensen dat zich *geen* zorgen maakt over privacy in rap tempo afneemt (van 44 % in 2013 naar 32 % in 2014); online winkels, sociale media en de Amerikaanse geheime dienst worden het minst vertrouwd en de Nederlandse belastingdienst het meest. De Eurobarometer stelde in 2011 vast dat 65 % van de Nederlandse burgers vindt dat de overheid 'meer en meer' persoonlijke informatie van hen vraagt. Mensen die veel online overheidsdiensten gebruiken, maken zich ook meer zorgen over hun privacy, en in het TNO rapport *i-Overheid, de burger in beeld* uit 2012 staat dat

[1] Dit essay is een bewerking van het rapport *Meer controle door burgers over hun persoonsgegevens*, door Liesbet van Zoonen en Heleen van der Meulen. Erasmus Universiteit Rotterdam, 2015. In opdracht van het Ministerie van Binnenlandse Zaken. Liesbet van Zoonen is Dean at the Erasmus Graduate School of Social Sciences and Humanities (EGS3H), Rotterdam Professor of Popular Culture, Erasmus University, NL Professor of Media and Communication, Loughborough University, UK. Website: liesbetvanzoonen.wordpress.com.

koppeling tussen uitkeringsgegevens en woongegevens, of tussen gemeentelijke gegevens en die van zorginstellingen tot een gevoel van onbehagen bij burgers over de overheid leidt.

Als je ons ernaar vraagt, zeggen we dus dat we ons grote zorgen maken over onze privacy, maar spontaan komt privacy als probleem niet bij ons op. We gedragen ons evenmin alsof privacy ons heel veel kan schelen. We zitten met 9 miljoen Nederlanders op Facebook en aanverwante platforms waar we met veel plezier ons privéleven met vrienden en familie delen, maar ook vaak met een groter publiek van onbekenden. Daarnaast geven we persoonlijke gegevens relatief makkelijk aan commerciële partijen als daar voordelen van gemak, kostenbesparing of efficiëntie tegenover staan. In de onmiddellijke nasleep van een aanslag vinden we het geen enkel probleem als de veiligheidsdiensten door onze data struinen; in levensbedreigende medische situaties vinden we het maar al te makkelijk als al onze gegevens al bij de hulpverleners liggen. Die discrepantie tussen zorg en zorgeloosheid staat bekend als de *privacy paradox*; de schijnbare tegenstelling tussen je zorgen maken over je privacy, maar er niet echt een probleem van maken en je gedrag niet aanpassen.

Een deel van die paradox is aan het verdwijnen; steeds vaker maken burgers, al dan niet georganiseerd, een probleem van privacy. Er zijn burgerinitiatieven zoals *Privacy First*, de *Privacy Barometer*, *VrijBit, Platform Bescherming Burgerrechten*, of *Stichting KDVP* (speciaal voor privacy in de medische sector), en bedrijfsinitiatieven zoals *Privacy Waarborg* dat een keurmerk voor het zorgvuldig gebruik van klantgegevens uitgeeft. Maar het is pas recent dat er ook iets van brede maatschappelijke onrust is te bespeuren. Dat bleek bijvoorbeeld toen de Volkskrant in oktober 2014 berichtte: “Burger wordt straks doorgelicht zoals profiel van crimineel wordt opgesteld”. Het artikel ging over de plannen van de Nederlandse overheid om persoonsgegevens uit verschillende databestanden te koppelen, teneinde uitkerings- en belastingfraude tegen te gaan. Al had de Tweede Kamer unaniem met het voorstel ingestemd, en lag een controverse dus niet voor de hand, toch deed het bericht onmiddellijk alarmbellen rinkelen. Andere media pikten het snel op, onder andere met de kop “Crimineel profiel van elke burger”[2]; diverse commentatoren spraken hun bezorgdheid uit. Minister Asscher voelde zich gedwongen om binnen een dag tekst en uitleg te geven via de site van de Rijksoverheid.

Maatschappelijke onrust ontstond ook toen de ING begin 2014 bekend maakte betalingsgedrag van hun klanten aan commerciële partijen door te willen geven, zodat deze gerichte persoonlijke advertenties kunnen aanbieden. “Een tuincentrum wil graag weten dat je elk jaar in maart 150 euro uitgeeft aan tuinspullen. Hij kan dan op het juiste moment een scherp aanbod doen,” aldus de bank. Ook in dit geval brak een storm van kritiek los, en volgens een snel uitgevoerde studie van het TV

[2] http://www.crimesite.nl/crimineel-profiel-van-elke-burger/

programma Radar, zorgde het plan ervoor dat bijna 80 % van de ING klanten minder vertrouwen in de bank hadden gekregen. Een derde van de ondervraagden zei te overwegen naar een andere bank over te stappen.[3] De ING probeerde de schade nog te herstellen met extra informatie, en stuurde een open brief naar haar klanten. Het mocht niet baten; het tumult ging pas liggen toen ING bekend maakte voorlopig van de proef af te zien.

We maken ons dus zorgen over onze privacy, en maken er steeds vaker een probleem van, maar wat kunnen we er zelf eigenlijk aan doen? Om die vraag te beantwoorden moeten we eerst vaststellen dat privacy als 'ideaal' aan het veranderen is.

Van privacy naar datacontrole

Vraagstukken over privacy gingen vroeger over het recht om het eigen privéleven af te schermen tegen de buitenwereld, en in het bijzonder tegen de overheid. Aan het einde van de 19e eeuw zorgde de opkomst van de massapers ervoor dat deze discussie over privacy uitgebreid werd met de vraag of en in hoeverre de journalistiek mocht berichten over privéhandelingen, gedachten en emoties van burgers. Dit kwam in de jaren daarna steeds sterker naar voren ten gevolge van een de opkomst van gespecialiseerde celebrity-media die berichten over het privéleven van sterren uit de sfeer van entertainment, sport en politiek. De meest recente aflevering van dit privacy discours betreft het *News of the World* schandaal in Engeland in 2011. De tabloid-krant van die naam moest sluiten vanwege het afluisteren van politici, royalty, slachtoffers van misdaad en andere nieuwswaardige figuren. Het leidde eveneens tot een onderzoek naar de praktijken van andere tabloids en een heftig openbaar debat over persvrijheid versus privacy.

Dit relatief simpele privacy paradigma is gebouwd op een scherp onderscheid tussen de intimiteit van het huiselijke, privéleven en de openbaarheid van ofwel de staat ofwel de massamedia. Met de opkomst van het internet hebben wetenschappers geopperd om ook persoonlijke communicatie, data, ervaringen, locatie en vereniging onder het klassieke privacybegrip te brengen en af te schermen voor externe partijen. Zo'n notie van privacy als afscherming is om verschillende redenen echter niet meer haalbaar. Voor online transacties is de uitwisseling van persoonlijke data met andere individuen of instanties noodzakelijk, en al die data zwerven inmiddels ook rond; naar het schijnt, zijn van het gemiddelde individu zo'n 1500 gegevens in verschillende databases opgeslagen. Als we online iets kopen, *moeten* we onze gegevens uitwisselen. Een leven off-the-grid, waarin je in geen enkel online netwerk opereert, is nog wel mogelijk, maar vreselijk onpraktisch. Bovendien is er

[3] http://www.radartv.nl/nieuws/archief/detail/article/30-ing-klanten-overweegt-overstap-1/

een hele nieuwe economie en cultuur van 'delen' in ontwikkeling, die gebouwd is op het uitwisselen van persoonlijke gegevens. Dat heeft niet alleen betrekking op sociale media waar we onze alledaagse of professionele besognes delen, maar ook op het uitwisselen van huizen, auto's, eten, gereedschap en noem maar op. In die nieuwe economie kan je niet meedoen als je je persoonlijke gegevens wilt afschermen (ik wil mijn huis wel ruilen, maar je mag niet weten waar ik woon……).

Een dergelijk afschermingsideaal in combinatie met volledige anonimiteit past niet meer bij een modern bestaan waarin online transacties en sociale media steeds vaker als eerste levensbehoeften worden gevoeld. De nieuwe Europese richtlijn over privacy is daarom gebouwd op de notie van *controle* over je data, wat onder meer inhoudt dat je moet kunnen inzien welke data een organisatie over je heeft, en moet kunnen corrigeren als dat nodig is. Zo kan je via MijnOverheid.nl inmiddels inzien over welke data de BRP, het UWV, je gemeente, het kadaster, de SVB, de RDW, de dienst Toeslagen, de WOZ, DUO, de donorregistratie, je pensioenverzekeraar en het LBIO[4] beschikken. De meeste commerciële organisaties bieden vergelijkbare 'MijnData' inzages; recentelijk kwam Google zelfs met een MyAccount waarop naar het schijnt werkelijk al je Google-data-gedrag terug te vinden is. Een tweede element van de nieuwe richtlijn betreft het recht dat je je data moet kunnen meenemen van de ene organisatie naar de andere; wie van bank wisselt krijgt daar bijvoorbeeld mee te maken. De derde en veel besproken vorm van datacontrole die de nieuwe richtlijn mogelijk maakt, betreft het recht om online ' vergeten te worden'. Dat heeft al tot meer dan 30 miljoen verzoeken aan Google geleid om links naar persoonlijke informatie te wissen.

In het huidige privacybegrip is 'controle' dus minstens even belangrijk geworden als ' afscherming'. In het verlengde van deze nieuwe focus op controle, ligt de vraag naar eigendom. Van wie zijn al die persoonlijke data eigenlijk? Gedeeltelijk komt deze vraag voort uit het feit dat de data-industrie inmiddels miljarden verdient met de verzameling en analyse van persoonlijke data waarmee consumentenprofielen worden gemaakt die voor veel geld aan de hoogste bieder worden verkocht. Waarom, is de logische verzuchting, zien wij zelf niks terug van dat geld? Het zijn toch onze data? De bedragen die zo verdiend kunnen worden, variëren nogal: Shawn Buckles, een Groningse student, verkocht zijn persoonlijke data aan de hoogste bieder en kreeg er 350 euro voor. De Financial Times biedt een online instrument aan waarmee je de waarde van je persoonlijke data kunt berekenen, en komt voor een dataprofiel van een gemiddelde huizenbezitter met thuiswonende kinderen op 35 cent uit. Ook zijn er start-ups geweest die het mogelijk maakten dat je zelf je data direct aanbiedt aan geïnteresseerde partijen maar geen van deze heeft een succesvol kostenplaatje weten te

[4] Basis Registratie Personen; Uitvoeringsinstituut Werknemers Voorzieningen; Sociale Verzekering Bank; Rijksdienst voor het Wegverkeer; Waardering Onroerende Zaken; Dienst Uitvoering Onderwijs; Landelijk Bureau Inning Onderhoudsbijdragen.

ontwikkelen. Een nieuwe social media site (Teckler) die beloofde 70% van hun inkomsten (uit het gebruik van data die door de bezoekers van de site waren aangeleverd zoals artikelen of foto's) te delen met zijn gebruikers, heeft het ook niet gehaald.

Al lijkt er vooralsnog dus nog weinig winst te behalen uit de exploitatie van je eigen gegevens, dat maakt de kwestie van data-eigendom niet minder pertinent, bijvoorbeeld vanwege de vraag wat er met email accounts, sociale media profielen, klantenkaarten en andere online gegevens moet gebeuren na je dood. Er worden hier inmiddels talloze diensten voor ontwikkeld met aansprekende namen als Death Switch, Suicide Machine of Accountkiller, en – iets minder spectaculair – Digizeker, een dienst van de Nederlandse notarissen waarmee 'nabestaanden jouw profielen van internet kunnen verwijderen'. Het betreft een digitale kluis waarin alle digitale gegevens van de gebruiker opgeslagen kunnen worden, en waarvan de notaris een 'reservesleutel' bezit die de erfgenamen kunnen gebruiken om de digitale nalatenschap af te ronden.

Er zijn steeds meer commerciële aanbieders van dergelijke 'kluizen', ook voor ons nog levenden. Het idee erachter is sympathiek: je houdt al je data bij je in je kluis, zodat ze niet onbeheerd over het internet zwerven. Wil iemand iets van je weten, dan geef je even inzage en doet daarna de kluis weer op slot; een soort Dropbox - maar dan veiliger - voor je persoonlijke gegevens. Maar, zoals *Bits of Freedom* zegt, door je gegevens in een digitale kluis te stoppen, geef je ze eigenlijk alsnog uit handen, namelijk aan het bedrijf dat de kluis aanbiedt. Bovendien ontstaat er een ander probleem, namelijk een controleparadox.

Van privacyparadox naar controleparadox

Dat burgers behoefte aan controle over hun persoonlijke data hebben, is wel duidelijk. We willen zien welke data er over ons circuleren, we willen kunnen ingrijpen als data niet kloppen of een vertekend beeld van ons geven, we willen zelf beslissen met wie onze data gedeeld worden. Een platform als Facebook geeft die illusie en als je mensen die illusie afneemt, worden ze boos, zoals in 2006 bleek. Tot dan toe waren de status-updates van Facebookgebruikers alleen zichtbaar voor degenen die jouw pagina bezochten. Via de nieuwe 'news feed' kwamen status updates automatisch bij al je vrienden terecht, die van elke nieuwe update op de hoogte werden gesteld. Veel mensen wilden dat niet en werden daar boos over. Zij hadden het gevoeld dat de controle over hun data hen afgenomen was, al veranderde er strikt genomen niets aan de openbaarheid ervan. Ander, Amerikaans, onderzoek suggereert ook dat mensen graag zelf bepalen aan wie, wanneer en hoe ze hun data vrijgeven. Als die data dan eenmaal vrijgegeven zijn, vermindert hun interesse in wat er daarna met die data gebeurt; sterker nog, ze worden dan regelrecht onvoorzichtig. Dat komt

misschien omdat vrijgeven iets is wat je zelf doet, en zichtbaar voor je is, terwijl toegang en gebruik door derden later plaatsvindt en ook niet merkbaar is. Controle over je eigen data, kan dus tot een pervers effect leiden: een groter gevoel van veiligheid produceert onveiliger gedrag. We wisten dat eigenlijk al uit het gedrag van autorijders: op goed verlichte, brede rijbanen rijdt men roekelozer dan op hobbelige donkere weggetjes.

Je zou dus kunnen denken dat we onszelf massaal voor de gek houden. De mensen die hun privacyzorgen omzetten in beschermend gedrag gebruiken misschien wel anti-spy en anti-spam software, halen cookies weg en checken de veiligheid van websites. Sommige mensen stappen zelfs over naar Torbrowser, die het mogelijk maakt te surfen zonder je IP-adres achter te laten. Het is alleen volstrekt onduidelijk of dat soort maatregelen wel echte controle oplevert. Ook doorgewinterde internetgebruikers en experts hebben eigenlijk geen idee waar ze precies toestemming voor geven als ze – na grondige lezing – instemmen met een privacystatement. Niet met dergelijke voorwaarden instemmen is overigens geen keuze, want dan kan je ook niet van de dienst gebruik maken. Allerlei recente browserapps die je kunnen laten zien welke derde partijen meekijken bij je surfgedrag helpen evenmin: je ziet bijvoorbeeld wel dat Google-analytics overal op aangesloten is, maar wat ze precies met je surfdata doen, is onduidelijk. Experts weten al nauwelijks meer wat er in de binnenkant van al die datasystemen gebeurt, laat staan een gewone burger. Bovendien zijn er allerlei datasystemen waar we als burger niet actief aan meedoen, maar waarin we wel geregistreerd worden, zoals bijvoorbeeld Closed Circuit Television (CCTV) en de monitoring van verkeersstromen. Het is daarom een illusie te denken dat we als burgers ooit nog *vooraf* controle kunnen uitoefenen over de data die over ons verzameld worden. Niet alleen vergt dat een onmenselijk goed georganiseerde en competente burger, maar ook vergt dat een begrip van systemen zoals Google-analytics dat maar voor een heel select en beperkt groepje mensen is weggelegd. Het is ook maar de vraag of al het onderzoek dat momenteel gedaan wordt om burgers en consumenten beter en gemakkelijker te informeren over hun privacy-opties wel de juiste oplossingen kan bieden. In het tijdperk van de complexe algoritmes, is iedereen, van leek tot expert, onvermijdelijk altijd te laat.

Algemeen Periodieke Data-Keuring

Er moet daarom een heel ander scenario bedacht worden dat we kunnen begrijpen door een vergelijking met de auto te maken. Ons wegennet zit propvol, maar als infrastructuur is het goed onderhouden en veilig. Wel is een rijbewijs verplicht, en een bewijs dat de auto rijwaardig is. Maar niemand verwacht dat we permanent weten of de auto in picobello staat is, en als er onderweg iets

kapot gaat of we aangereden worden, verwacht niemand dat we terplekke de auto kunnen repareren; dan bellen we de wegenwacht. Bekijken we data op die manier, dan is de reden dat we ons zorgen maken niet dat onze data ergens ongecontroleerd 'rondrijden', maar dat we bang zijn voor datapech, dataongeluk of datacrash: als een slecht willende ex-partner je privéfoto's naar zijn vrienden doorstuurt; als bedrijven je ongewenste reclame sturen door de brievenbus of via internet; als een oplichter op jouw naam spullen bestelt; als je verkeerd geprofileerd wordt door de grenscontrole en als mogelijke terrorist aangemerkt wordt; als de uitkeringsinstantie je geld intrekt omdat volgens de gemeentelijke basisadministratie de vorige bewoner nog op je adres staat ingeschreven; als het UWV een jaar van je arbeidsverleden mist; als je op basis van naamsverwisseling in Guantánamo Bay belandt; als iemand zijn laptop met databestanden in het café laat liggen, en ga zo maar door. Voor een nog uitgebreider scala aan nare voorbeelden raadplege men de rapportages van de Nationale Ombudsman. We zijn niet bang voor de auto, maar voor wat ermee kan gebeuren. Zo zijn we ook niet bang voor data, maar voor de foute dingen die ermee kunnen gebeuren. Als we daar nu eens iets aan konden doen? Als we een APK en een datawacht voor onze persoonsgegevens invoeren, zijn we in één klap van de paradoxen af. Dan hoeven we burgers niet langer te belasten met het onderhoud van hun data; hij of zij kan vrijgeven wat ze maar wil, en laat jaarlijks controleren of alles nog deugt, en of er geen onterechte verbindingen tussen databestanden gemaakt zijn. Dat geeft ruimte aan een nieuw midden-en kleinbedrijf van data-garages die jaarlijks of tweejaarlijks inventariseren waar en met wie je data rondzwerven, checken of alles nog in orde is en indien nodig reparaties verrichten. Daarbij gaan we ervan uit dat er altijd wel ergens op de snelweg iemand met pech komt te staan, en in dat geval rukt de data-wacht uit. Wie zich niets bij die metaforen kan voorstellen, denkt eens aan de bank die je opbelt als er verdachte transacties met je credit card plaatsvinden. Zo'n bank heeft misschien wel de veiligste systemen die er zijn (privacy-by-design), gebruikers zijn relatief voorzichtig en worden bovendien jaarlijks gedwongen om nieuwe veiligheidsmaatregelen aan te maken. Toch gaat er dan nog steeds wel eens iets mis, en is er het vangnet van de mondelinge, persoonlijke controle. Die bank heeft als model eigenlijk een APK (jaarlijks nieuw wachtwoord aanmaken) en een wegenwacht (uitrukken bij pech).

Er is vast heel veel tegen dit idee in te brengen, en er zit ook een nog onbesproken en misschien wel onoplosbaar scala aan uitvoeringsproblematiek in; wie stelt de kaders voor die APK? Gaat het over alle data of alleen die van de overheid? Is zo'n datagarage misschien een nieuwe privacy bedreiging? Maar het ging mij er vooral om te laten zien dat vooraf controle krijgen en houden over je data vrijwel niet meer mogelijk is, en dat er daarom vaker gedacht moet worden aan mechanismen die ingrijpen *achteraf* mogelijk maken. Zulke herstelmechanismen achteraf halen een hoop druk en

onmogelijke verantwoordelijkheid bij de burger weg, ze geven vertrouwen in de snelweg, en ze creëren nieuwe bedrijvigheid. Wat willen we nog meer?

Gebruikte bronnen:

ECP (2014). Online gemak belangrijker dan privacy. Onderzoeksrapport Platform voor de Informatiesamenleving. http://ecp.nl/actueel/4288/online-gemak-belangrijker-dan-privacy.html.

Eurobarometer, S. (2011). *Attitudes on data protection and electronic identity in the European Union."* Brussels: European Commission, Directorate-General for Communication. Special Barometer 359.

The Guardian (2014). How much is personal data worth? http://www.theguardian.com/news/datablog/2014/apr/22/how-much-is-personal-data-worth