Privacy in de digitale wereld

1. Buiten komt binnen

De introductie van de telefoon veroorzaakte opwinding in het leven van grootmoeder, vertelt de Utrechtse antropoloog Ton Robben. Het was natuurlijk geweldig om de stem van iemand ver weg te kunnen beluisteren via dat toestel van zwart bakeliet in de gang. Maar soms was grootmoeder niet klaar voor de buitenwereld. Dan zei ze: 'Ik kan nu de telefoon niet opnemen, want ik heb mijn haren niet gekamd.'

De telefoon bracht plotsklaps de buitenwereld grootmoeders huis binnen, en daarmee begonnen vertrouwde categoriën te wankelen. Daarin stond Robbens grootmoeder niet alleen. Zo beschrijft de kleine Walter Benjamin de opschudding die ontstond toen rond 1900 de telefoon doordrong in het burgerlijke Berlijnse huishouden waar hij opgroeide: "Weinigen van ons die het apparaat gebruiken, weten wat een verwoesting het ooit teweegbracht in de familiekring. Het geluid waarmee de telefoon rinkelde tussen twee en vier 's middags, als een schoolvriendje met me wilde spreken, was een alarmsignaal dat niet alleen het middagdutje van mijn ouders bedreigde, maar de hele historische periode die deze siesta behelsde. (...) Indertijd hing de telefoon – een verschoppeling achteloos geplaatst tussen de wasmand en de gasmeter – nog steeds in de hoek van de gang achter, waar zijn gerinkel de verschrikkingen van het Berlijnse huishouden vermenigvuldigde. Als ik, na met grote moeite mijn zintuigen de baas te zijn geworden en na een struikeltocht door de sombere gang, aankwam om het oproer te sussen, trok ik de twee ontvangers eraf, die zwaar waren als halters, stak mijn hoofd ertussen, en was onverbiddelijk overgeleverd aan de stem die nu klonk. Er was niets dat het geweld kon stillen waarmee die tot mij doordrong. Ik leed machteloos, constateerde dat die stem mijn besef van tijd uitwiste, mijn ferme voornemens, mijn plichtsgevoel. En net zoals een medium de stem gehoorzaamt die vanuit het graf bezit van hem neemt, zo onderwierp ik me aan het eerste het beste voorstel dat via de telefoon tot mij kwam."[1]

Het zijn heftige bewoordingen die Benjamin kiest: via de telefoon dringt de buitenwereld op gewelddadige wijze je privéwereld binnen, zet daar de ordening op haar kop, en je weet niet hoe je je moet verweren tegen die verzoeken en impulsen van buitenaf. Het is maar de vraag of we er, ruim een eeuw later, zoveel beter voor staan. Weten wij goed verschil aan te brengen tussen privé en publiek als het op informatie- en communicatietechnologie aankomt? Zijn wij als gebruikers van die

[1] Walter Benjamin, *Berlin childhood around 1900*, Harvard University Press, 2006, p. 49-50 (mijn vertaling).

technologie autonome actoren, of zijn ook wij teveel onder de indruk van een stem van gene zijde om te beschermen wat tot onze innerlijke kern behoort?

Het is nu eens niet overdreven om te stellen dat informatie- en communicatietechnologie onze leefwereld de afgelopen decennia revolutionair heeft veranderd. Communicatie is veel minder aan ons lichaam gebonden dan vroeger; preciezer gezegd, technologie draagt de signalen die je lichaam uitzendt potentieel de hele wereld over. Dat is prachtig, handig, bevrijdend en opwindend. Maar ook verwarrend. We zijn er eigenlijk nog niet echt aan gewend. Als je belt, blijft de toestand van je kapsel verborgen, weten we nu. Maar andere signalen kunnen, bedoeld én onbedoeld, wel worden opgepikt door vreemden. Wat zend je nu precies uit, en wat gebeurt er met die informatie?

2. Buiten is binnen

Kort geleden zat ik ’s avonds in de trein op weg naar huis. Schuin aan de overkant van het gangpad was een jonge vrouw druk aan het bellen. Een vriendinnengesprek – kletserig, vertrouwd. ‘Moet je nou horen, die jongen tegenover me is uit zijn neus aan het eten, goor hé!’, vertelde ze lacherig tegen haar vriendin. Waarop de jongeman kwaad zei: ‘Ik hoor wel wat je zegt hoor!’ Het meisje, misschien misleid door de oortjes die hij in had, probeerde eroverheen te lachen, maar gezellig werd het niet meer. Deze twintigers voelden zich allebei te kijk gezet.

Het heet dat twintigers vertrouwd, haast vergroeid, zijn met communicatietechnologie. Toch besefte dat bellende meisje kennelijk niet wat ze precies uitzond, en naar wie. Dat was misschien nogal onnozel – die jongen zat recht tegenover haar – maar geeft ook een psychologisch inkijkje: als dit meisje belt, lijkt de publieke ruimte voor haar niet te bestaan. Het is een onaangename schok als blijkt dat de buitenwereld mee kan luisteren met haar intieme uitwisselingen. Dat had dit meisje kunnen weten. In de woorden van Ton Robben: “Zodra je een communicatiekanaal openzet, ben je niet alleen een ontvanger, maar ook een zender van informatie, of je nu wilt of niet - je hebt niet de volle controle over de rol die je vervult.” Zelfs niet als de buitenwereld voor haar zit, in de vorm van die neuspeuterende jongen. Daar staat tegenover dat de mogelijkheden van de digitale communicatie niet stroken met onze lichamelijke aanleg. Voorheen vereiste communicatie altijd lichamelijke aanwezigheid. In het digitale tijdperk is coummunicatie onthecht geraakt van het lichaam, en dat zet oeroude, impliciete aannames op zijn kop. Dat is flink wennen.

Informatietechnologie brengt plezier en gemak, contact en voorspoed. Maar doet ons ook zeggenschap verliezen over wat we van onszelf tonen, en aan wie. Met andere woorden: je kunt zelf

niet meer zo goed bepalen wat je openbaar wilt maken, en wat je voor jezelf wilt houden. Door informatietechnologie komt je privacy in het geding.

3. Wat bedoel je met privacy?

De *Verklaring van de Rechten van de Mens* beschermt privacy expliciet, en wel in artikel 12. 'Niemand zal onderworpen worden aan willekeurige inmenging in zijn persoonlijke aangelegenheden, in zijn gezin, zijn tehuis of zijn briefwisseling, noch aan enige aantasting van zijn eer of goede naam. Tegen een dergelijke inmenging of aantasting heeft een ieder recht op bescherming door de wet', luidt dat artikel[2]. Daarmee erkent de Verklaring expliciet één van de pijlers van het klassieke burgerlijk-politieke recht. Van oudsher is het recht op privacy bedoeld om de verhouding tussen burger en staat te regelen. Burgers zijn kwetsbaar. Door een deel van hun souvereiniteit over te dragen aan de staat – met name door de staat het monopolie op geweld te geven - wordt de staat potentieel gevaarlijk voor diezelfde burgers. De privacy-clausule van het 'contract' tussen staat en burgers moet ervoor zorgen dat de staat niet té machtig wordt en zich verre houdt van de inmenging in het privéleven van burgers.[3] Wat zich binnen de besloten ruimte van het huis afspeelt, gaat 'buiten' niets aan.

De informatie- en communicatietechnologie die de wereld sinds enkele decennia overspoelt, heeft dit contract echter op losse schroeven gezet. Wij burgers zetten de communicatiekanalen zelf wijd open. En de staat vertoont de sterke neiging om bestanden met onze persoonsgegevens aan elkaar te koppelen om ons 'beter van dienst' te zijn. Buiten komt binnen, en binnen wordt buiten. Daarmee blaast ICT de vertrouwde, aan ons lichaam gebonden manieren van interacteren als het ware op. Vanwege de digitale revolutie lopen binnen en buiten op een volstrekt nieuwe manier door elkaar heen, en, we weten we nog niet waar ons dat eigenlijk laat. Gezonde omgangsvormen met deze nieuwe situatie hebben zich nog niet uitgekristalliseerd. Ondertussen lijken we, duizelig van de mogelijkheden als we zijn, niet goed meer te beseffen wat privacy nu eigenlijk beoogt te beschermen.

4. Technologie leidt tot function creep

Privacy in het digitale tijdperk betekent in ieder geval *niet* dat de dingen die je in de private sfeer doet ook onopgemerkt blijven. Ieder van ons is vandaag al op tal van manieren geregistreerd. Veiligheidscamera's en GPS-apparatuur maken het mogelijk om de route te reconstrueren die je

[2] Bron: website Office of the High Commissioner for Human Rights.

[3] Behalve als burgers privé gewelddadige acties bekokstoven die de veiligheid van andere burgers zouden aantasten. Dan kan –op last van de rechter- het recht op privacy van deze burgers 'overruled' worden. Dit is de bron van de zo vaak gesignaleerde spanning tussen privacy en veiligheid.

vandaag hebt afgelegd. Je elektronische sleutel heeft je aangemeld op je werk, je aankopen zijn geregistreerd via klantenkaarten, je surfgedrag wordt opgeslagen en geanalyseerd, je lichaamsfuncties worden wellicht bijgehouden via apparaatjes die je op je lichaam draagt.

Al die technologie is je dagelijkse leven binnengekomen met de belofte dat zij jouw doelen dient. En dat doet ze natuurlijk ook. Technologie doet echter al snel méér dan ze belooft. Ze wordt ontwikkeld voor een bepaald doel, maar vindt in de loop der tijd een bredere toepassing. Een bekend voorbeeld van het fenomeen, ook wel 'function creep' genoemd, zijn uitvindingen voor de ruimtevaart die later een bestemming vonden in de anti-aanbaklaag in pannen, de draadloze boormachine en sportschoenen met lucht in de zolen.[4] ICT is zelf een uitgesproken voorbeeld van die verruiming van toepassingen: het internet werd eind jaren zestig ontwikkeld door het Amerikaanse ministerie van Defensie met als doel om een manier van informatieuitwisseling te ontwikkelen die zelfs bij een nucleaire aanval nog betrouwbaar zou zijn. Nu synchroniseren we onze gezinsagenda's via het internet. Die toepassing is bepaald niet van tevoren bedacht. Regie over zo'n ontwikkeling is er nauwelijks, en komt hoe dan ook eerder van de R&D-afdeling van technologiebedrijven dan vanuit de publieke sfeer.

Het netwerkkarakter van informatietechnologie maakt het buitengewoon aantrekkelijk om systemen met verschillende functies aan elkaar te koppelen en werkt aldus 'function creep' extra in de hand. Jurist en WRR-lid Corien Prins memoreert hoe het burgerservicenummer (BSN) aanvankelijk fungeert als 'sleutel' voor het veilig uitwisselen van persoonlijke gegevens tussen burger en overheid. 'Inmiddels wenst een groeiend aantal partijen in de private sector ook gebruik te mogen maken van dit nummer en – in sommige gevallen – tevens van de aan dit nummer verbonden persoonsgegevens', schrijft Prins. Binnen de zorg mag het BSN nu al worden gebruikt.[5] Gebruikersgemak is een sterk argument voor het koppelen van bestanden. Maar door het koppelen van bestanden *verandert* het gebruik van de informatie, vaak zonder dat de oorspronkelijke afspraken tussen de leverancier en de ontvanger van informatie worden herzien.

Daar komt bij dat de technologie informatie dermate snel kan verzamelen en in zulke onvoorstelbare hoeveelheden kan beheren, dat die verzamelde informatie als het ware zelf een aparte entiteit wordt, die te 'ontginnen' is door organisaties die toegang hebben tot die informatie. Het gebruik van de informatie over personen zingt daarmee verder los van de redenen die deze personen ooit hadden om informatie te verstrekken. *Als* zij al toestemming hebben gegeven – veel informatie over het gedrag van personen wordt inmiddels routineus verzameld en opgeslagen. De Utrechtse hoogleraar Intelligence and security studies Bob de Graaff zegt: "Je geeft van alles over

[4] De voorbeelden staan genoemd in 'Justitiële Verkenningen' jrg. 37, nr. 8 (2011), een special over function creep en privacy.
[5] Zie Prins' artikel in 'Justitiële Verkenningen', op.cit.

jezelf prijs, of je nu wilt of niet. Je bent een bekeken mens." Een klein deel van de mensen, 'zeg 2 procent', gaat daar vervolgens rekening mee houden. Zij pinnen niet maar gebruiken contant geld, weigeren een bonuskaart, kopen een papieren treinkaartje, shoppen niet in webwinkels, et cetera. De Graaff: "Met dat gedrag spelen ze zichzelf in feite in de kijker – dat is zó afwijkend van het patroon!"

Veiligheid is een andere, sterke reden om bestanden te koppelen en informatie te screenen. De angst voor terrorisme zit er goed in en is ook niet denkbeeldig, zoals het wereldnieuws geregeld bewijst. Het beschermen van burgers is een zeer basale taak van de overheid, die ook verankerd is in de *Verklaring van de Rechten van de Mens*. De overheidstaak om de collectieve veiligheid zo goed mogelijk te garanderen is dermate belangrijk dat de wet voorziet in de mogelijkheid om andere rechten van burgers daartoe soms opzij te schuiven. ICT lijkt ongekende mogelijkheden te bieden om die overheidstaak uit te voeren. Potentiële terroristen moeten immers informatie vergaren en hun daden voorbereiden en laten daarbij vrijwel onvermijdelijk digitale sporen na. De drang om het digitale verkeer na te pluizen op 'verdachte patronen' in de hoop op die manier terroristen te pakken vóórdat ze toeslaan, is dan ook groot.

Maar deze nieuwe manier om de veiligheid van burgers te willen garanderen, raakt aan het klassieke mensenrecht op privacy – zoveel wordt wel duidelijk uit de recente rel rond het optreden van de National Security Agency (NSA), de inmiddels overbekende Amerikaanse militaire inlichtingendienst. De uitwisseling van informatie tussen burgers, organisaties, regeringen – die tegenwoordig veel vaker wel dan niet een elektronische vorm aanneemt - blijkt routineus te worden opgepikt door inlichtingendiensten. De NSA blijkt rechtstreeks toegang te hebben tot de netwerken van onder meer Facebook, Google, Skype, Apple, Yahoo en YouTube – zonder dat de gebruikers van Facebook *et cetera* daar weet van hadden. De Nederlandse tegenhanger van de NSA, de Militaire Inlichtingen- en Veiligheidsdienst (MIVD) gebruikt deze data ook; de MIVD laat zelfs zónder rechterlijke toestemming zoekmachines op deze gegevens los om potentiële verdachten te identificeren.[6] Telecom- en internetproviders moeten in Nederland elke dag hun gegevens overhevelen naar het Centraal Informatiepunt onderzoek Telecommunicatie (CIOT), zoals IP-adressen, e-mailadressen, lijsten met eigenaren van websites. Politie, Landelijk Parket, Rijksrecherche, inlichtingendiensten en nog wat organisaties mogen, onder voorwaarden, vragen stellen aan het CIOT. In 2012 deden ze dat 2,7 miljoen keer.[7]

In haar drang om de veiligheid van burgers te garanderen wroet de overheid dus tamelijk routineus in de persoonlijke gegevens van diezelfde burgers. De afgeluisterden krijgen geen helder

[6] Tom-Jan Meeus, 'Onrechtmatige spionage die we even wegstoppen', *NRC Handelsblad* 15 juni 2013.

[7] Carola Houtekamer, 'Wat weet Nederland van u?', *NRC Handelsblad* 15 juni 2013.

inzicht in de agenda van die diensten, en weten dus ook niet wat dergelijke informatie in de ogen van die schimmige ontvangers kan gaan betekenen. We verliezen grip op hoe we verschijnen. Hoe deze praktijken te verantwoorden zijn binnen de kaders van de Grondwet is een open vraag, die urgenter is geworden door de internationale rel rond NSA.

5. Big Data verandert onderzoeksmethoden

Het principiële debat over de mate waarin privacy mag worden opgeofferd aan veiligheid, zal voorlopig nog niet verstommen. Dat laat een meer pragmatische vraag open: hoe effectief is het eigenlijk om grote digitale bestanden te screenen in de verwachting zo terroristen op te sporen? Dit is impliciet ook een vraag naar proportionaliteit: is de veiligheidswinst van deze praktijken groot genoeg om de bijbehorende privacyschendingen te rechtvaardigen?

Dat valt, althans halverwege de jaren 2010, te betwijfelen. De mogelijkheden van het ontginnen van *Big Data* lijken (semi-)overheidsdiensten naar het hoofd te stijgen. De diensten hebben nog zo weinig ervaring met deze nieuwe technologieën opgebouwd dat ze nauwelijks overzien wat ze aan het doen zijn. Bob de Graaff: “Politie en justitie hebben zelf niet zoveel gespecialiseerde kennis over data-mining in huis. Als iemand een geweldige nieuwe opsporingsmethode bij hen komt pluggen, denken ze al snel: ‘Wauw’! Zo’n product is hen relatief gemakkelijk aan te praten. Ook al omdat de politiek vooral wordt afgerekend op aanslagen die ze missen, en dus op zeker wil spelen.”

De Graaff heeft gezien hoe deze trend richting data-mining en patroonherkenning tot flinke veranderingen op de werkvloer leidde. “Het oude inlichtingenwerk ging aan de slag vanuit een werkhypothese. Onderzoekers gingen ervan uit dat ze vanzelf op ongerechtigheden zouden stuiten als zij slim gegevens zouden combineren. Die werkhypothese wordt nu op zijn minst aangevuld met software die automatisch een bulk gegevens screent en de anomalieën, de extreme afwijkingen van een patroon, opmerkt. Door zulke grote hoeveelheden informatie te combineren kunnen er dus verbanden gelegd worden. Er rolt een beperkte sample ‘personen met afwijkend gedrag’ uit de computer, die inlichtingenwerkers dan extra gaan volgen.” Daarbij lijken we op de koop toe te nemen dat inlichtingenvergaring en politieel-justitiële vervolging in elkaar lijken te vervloeien. In de woorden van De Graaff: we nemen dus het risico dat de politie zich dreigt zich te ontwikkelen tot geheime politie.[8]

[8] Bob de Graaff, ‘Waterboarding, rendition, secret flights en secret prisons’, in *Contraterrorisme en ethiek*, Kowalski & Meeder, Boom, Amsterdam (2011), p18.

Data-mining is duur. Volgens De Graaff kost het opbouwen van zelfs maar een klein databestand voor data-mining al snel een paar miljoen, deels omdat vervuilde bestanden moeten worden opgeschoond. Data-mining kan ook *gevaarlijk* zijn, met name als informatie veel sneller groeit dan ons begrip van hoe we die informatie moeten beheren, stelt Nate Silver, de jonge statisticus en opiniepeiler die de Amerikaanse presidentsverkiezingen van 2012 foutloos voorspelde. In zijn boek *The Signal and the Noise*[9] maakt hij duidelijk waarom: het doet ons al snel geloven dat we signalen uit de data oppikken, terwijl we ons in feite laten leiden door ruis. De statistische wetenschappen duiden dit type vergissingen aan met de term 'overfitting'. 'Overfitting' wil zeggen dat je verbanden ontwaart in de verzamelde data zonder werkelijk op een onderliggende structuur in die data te zijn gestuit. Je hebt dus in feite ruis ontdekt. Dit gebeurt te goeder trouw, uit ijver, en vooral in situaties waarin de data veel ruis vertonen én het begrip van de onderliggende patronen zwak is.

'Stel dat je een statistisch model hebt dat bedoeld is om elf gebeurtenissen te verklaren, en dat je daarvoor moet kiezen uit vier miljoen gegevens', zegt Silver, 'dan zullen veel van de verbanden die je tussen die enorme hoeveelheid gegevens gaat vinden vals zijn'. Ofwel: er zullen dan tal van correlaties opduiken, maar die correlaties hoeven helemaal niets te betekenen te hebben. Ook al lijken de verbanden misschien suggestief. En ook al passen ('fitten') ze prima op de ruis in onze gegevens uit het verleden. Ter vergelijking: de teruggang van de ooievaarstand in Nederland in de jaren 1960 viel samen met de daling van het geboortecijfer, maar die samenhang betekent niets.[10] Het verband past met de data, maar verwijst niet naar een onderliggend patroon.

Precies dit mechanisme van 'overfitting' maakt volgens Silver de kans op foutieve voorspellingen in het tijdperk van *Big Data* groter. De hoeveelheid beschikbare informatie neemt exponentieel toe, en dat leidt tot een exponentiële toename van het aantal te onderzoeken hypotheses. Want als je zonder veel inzicht in onderliggende patronen zoekt in databestanden, zul je elke correlatie die er uit de data rolt welhaast moeten behandelen als hypothese. Maar: 'data bestaan grotendeels uit ruis, net zoals het universum grotendeels bestaat uit lege ruimte', aldus Silver.[11]

Daar komt nog een statistische wijsheid bij: met name als een gebeurtenis heel zeldzaam is (zoals een terroristische aanslag), dan kunnen vals-positieve uitslagen (ofwel: onterechte verdenkingen) al heel snel de uitkomsten overheersen. Want als een waar-positieve uitslag heel

[9] Nate Silver, *The Signal and the Noise: the Art and Science of Prediction*. Penguin, London (2012). De parafrases en citaten van Silver komen uit alle dit boek, steeds onze vertaling.
[10] Een onvergetelijk voorbeeld van de overleden Utrechtse psycholoog Piet Vroon.
[11] Silver, op.cit. p250.

zeldzaam is, dan kan het zo zijn dat - zeg - 80 procent van de waar-positieve uitslagen terecht als waar worden aangemerkt en 90 procent van de negatieve uitslagen terecht worden verworpen. In ons voorbeeld: 80 procent van de verdenkingen van terrorisme zou terecht zijn, en 90 procent van de mensen die niet van terrorisme worden verdacht, hebben ook geen plannen in die richting. Dit zijn cijfers waarvan de opsporings- en veiligheidsdiensten waar De Graaff op doelde vermoedelijk wel onder de indruk zullen zijn. En die cijfers kloppen, maar laten onverlet dat *tweederde* van alle personen die volgens dit algoritme van terrorisme worden verdacht daar *ten onrechte* worden verdacht.[12] Nogmaals: dit effect doet zich vooral voor in situaties waarin waar-positieve uitslagen zeldzaam zijn. Zoals, gelukkig, het aantal mensen dat serieus terroristische aanslagen voorbereidt.

Dit is te lezen als een argument om vooral ook te investeren in onderzoek naar de motieven en denkwijzen van potentiële terroristen – dergelijke kennis zal het zoeken in de ruis een stuk effectiever maken. Maar het is ook een waarschuwing. Mensen die serieus verdacht worden van het voorbereiden van een terroristische aanslag, krijgen met veel staatsgeweld te maken. Ze zullen worden opgepakt en op zijn minst hardhandig worden ondervraagd. En ook als de verdenking verder nog niet veel vlees op de botten heeft, kun je al aardig wat last ondervinden van het feit dat een algoritme jou als 'verdacht' aanmerkt. Bob de Graaff: "Stel dat jij Arabische poëzie bekijkt op internet, films over terrorisme leent en de afgelopen jaren drie keer naar Pakistan bent gereisd, dan kan dat genoeg zijn om jou extra te screenen. Zonder dat je daar zelf een idee van hebt. En dus zonder dat je het beeld dat instanties van je vormen, kunt corrigeren. Je merkt misschien dat je moeite krijgt om binnen de Verenigde Staten van de ene stad naar de andere te vliegen, zonder dat je begrijpt waarom." Met een (zeer) grote kans dat jouw burger- en politieke rechten geschonden zijn zonder enige veiligheidswinst voor de gemeenschap. Je had slechts de pech een vals-positiefje te zijn.

Data-mining lijkt veel op zoeken in het donker. Aan een zoekopdracht gaat zelden een doordachte hypothese vooraf – dat hoeft ook niet, want de beschikbare rekencapaciteit is toch enorm. In theorie kan dat ongerichte zoeken maken dat je op verrassende, baanbrekende verbanden stuit. Vaker echter leidt het tot absurde correlaties, waar geen levend mens serieus tijd aan zou besteden, maar die wel rood oplichten in de computer. De Graaff heeft een triviaal voorbeeld: "Voor een klein onderzoekje naar hoe digitale identiteit tot stand komt, hebben we enkele vrijwilligers gevraagd of we hun digitale bewegingssporen een tijdje in kaart mochten brengen. We vroegen ons af of we zo zouden kunnen achterhalen waar die vrijwilligers wonen. In één geval kregen we drie

[12] Zie de paragraaf 'The problem of false positives' in Silver (p249-251) voor een heldere uitleg en grafiek.

locaties: inderdaad het privé-adres, het kantooradres, én het verkeersknooppunt waar deze persoon heel vaak vaststaat."

De vraag is wat die gegevens in databestanden over jouw identiteit prijsgeven. De Graaff: "Zelf zou je misschien zeggen: 'Dat verkeersknooppunt zegt bar weinig over mij; wat echt belangrijk is en wat mij zinvol onderscheidt van anderen, blijft privé.'" Maar de zeggenschap over wat belangrijke kenmerken van jou zijn, ligt niet bij jou – en als het programma iets 'irrelevants' over jou aan het licht brengt, kun je daar toch flink last van hebben. Bovendien is het evengoed mogelijk dat alle inmiddels verzamelde en opgeslagen informatie méér van jouw persoonlijke identiteit prijsgeeft dan je lief is. De Graaff: "Je eerste huwelijk maakt voor altijd deel uit van jouw openbare identiteit, terwijl je zelf kan vinden dat je huidige identiteit fundamenteel anders is. En informatie kan je ook achtervolgen. Een collega van mij heeft jaren geleden een zeer fel stuk voor de opiniepagina van *de Volkskrant* geschreven, waarin zij tekeer gaat tegen mannen. 'Denk jij nog steeds zo over mannen', vroeg ik haar eens. 'Ik weet waar je naar verwijst', zuchtte ze. 'Ik was net gescheiden en woedend. Ik heb meerdere malen gevraagd of dat stuk van de site af mag, maar dat gebeurt dus niet.'" Ze gaat nu tegen wil en dank als mannenhaatster door het leven.

6. Digitale fouten corrigeren is moeilijk

Achtervolgd worden door een *faux pas* uit het verleden die een digitaal spoor nalaat in de openbare ruimte, is misschien nog te voorkómen door zelf beter op te letten en wat mediawijzer te worden. Maar als anderen welbewust met jouw officiële identiteit rommelen - de gegevens dus waarmee je je zaken regelt - dan sta je behoorlijk machteloos. Zeldzaam is dit niet. In 2012 waren er in Nederland 600.000 gevallen van identiteitsfraude; in totaal zijn inmiddels 2 miljoen mensen slachtoffer geworden van identiteitsfraude[13]. Vaak gaat het hier om het skimmen van een bankpas, maar in tien procent van de gevallen gebruikten kwaadwillenden andermans identiteit om straffeloos een overtreding of misdrijf te begaan.[14] Het is niet gemakkelijk om een foutief digitaal beeld te corrigeren dat van jou is ontstaan. Wat de computer zegt, wordt standaard als uitgangspunt genomen, en als de computer 'nee' zegt, is het als burger moeilijk om verhaal te halen. Bij wie, of welke instantie, zou je moeten aankloppen? De verantwoordelijkheid voor de juistheid van al die digitale persoonsgegevens is (nog) niet goed geadresseerd.[15] Corien Prins: "Het is op dit moment niet heel duidelijk wat eigenlijk een kwalitatief goede manier van het verzamelen van gegevens zou zijn, noch is duidelijk wie die kwaliteit zou moeten bewaken."

---

[13] Cijfers van het ministerie van Binnenlandse Zaken en Koninkrijkrelaties.
[14] Bron: *EenVandaag*, http://www.eenvandaag.nl/binnenland/46177/identiteitsfraude_neemt_toe
[15] Zo constateert bijvoorbeeld het WRR-rapport *iOverheid* uit 2011 van Corien Prins cum suis.

Simon Hania, informaticus en Corporate Privacy Officer van navigatiesoftwarefabrikant TomTom, heeft wel een idee waarom het aan die duidelijkheid ontbreekt. “ICT werkt binair. Uiteindelijk kom alles neer op nullen en enen, op ja-nee-vragen. Terwijl deze technologie functioneert binnen een complexe wereld vol nuances. Hoe integreer je die werelden? Dat is in de praktijk een probleem. Juristen hebben vaak bar weinig verstand van ICT; ze hebben een ander hoofd en zijn niet voor niets rechten gaan studeren. Informatici hebben weer weinig op met vragen die je niet met een duidelijk ‘ja’ of ‘nee’ kunt beantwoorden. Ze zijn sowieso vaak meer gericht op software en apparaten, waarmee ik zeg: ze zijn *niet* gericht op data. Laat staan op de effecten van *Big Data* op de wereld. In het IT-onderwijs is daar ook geen aandacht voor. Dus databeheer op internet is een soort vogelvrij gebied.”

7. Privacygevoelige informatie als bijvangst

TomTom ondervindt daar last van, zegt Hania. Het bedrijf bevindt zich in de eigenaardige situatie dat het beschikt over méér persoonlijke gegevens dan het lief is. Hania licht toe: “Op de ring rond Amsterdam mag je honderd rijden, maar iedereen weet dat je die snelheid op maandagochtend wel kunt vergeten. Bij TomTom maken we sinds 2008 een digitale kaart van het wegennet die de actuele situatie in een bepaald gebied weergeeft. Doel is om onze klanten een voorspelling te bieden van hun reële reistijd.” Daartoe moet TomTom de feitelijke snelheid van een significant aantal automobilisten kennen. Gebruikers van de service geven TomTom toestemming om via GPS meerdere malen hun positie vast te stellen. Zo kan TomTom uitrekenen hoe lang een bepaalde gebruiker doet over een bepaalde afstand, en dus hoe snel hij of zij kan rijden. Hania: “Als we dat van genoeg gebruikers weten, kunnen we aardig accurate voorspellingen doen.” *En passant* weet TomTom natuurlijk ook welk traject een bepaalde gebruiker aflegt. Voor het bedrijf is dat bijvangst, maar in principe heeft TomTom dus een grote database met de lokatiesporen van zijn gebruikers.[16] Hania: “Privacywaakhonden vinden dat gevoelige informatie, en dat snap ik. Door de trajecten die iemand aflegt te bestuderen, kun je in principe veel te weten komen over iemands religie, seksuele leven, gezondheid, noem maar op.”

De wetgeving over de bescherming van de persoonlijke levenssfeer van burgers[17] is op zichzelf vrij rechtoe-rechtaan, zegt Hania. Maar interpretatie en toepassing zijn schimmig. Hania weet niet altijd wat de wettelijke normen betekenen voor de IT-plannen van TomTom. Anders

[16] TomTom bewaart deze gegevens maximaal 24 uur op hun server, en knipt ‘onmiddellijk en onherstelbaar’ de naam van de gebruiker los van diens bewegingen, waardoor een traject dus niet meer aan een bepaald individu te koppelen is, aldus Hania. Zie ook het pr-filmpje http://www.tomtom.com/en_gb/safeguarding-your-data/

[17] Hania doelt op *Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens.*

gezegd: hij weet niet atlijd of TomTom zich nog binnen het kader van de wet beweegt. Hania: “Ik heb contact gezocht met het College Bescherming Persoonsgegevens, de Nederlandse toezichthouder op het handhaven van deze richtlijn, en heb hen gevraagd met ons mee te denken: kunnen we bepaalde richtingen inslaan, of zijn we dan illegaal bezig? Het CBP reageerde: ‘wij beoordelen te zijner tijd wel of het kan’. Met andere woorden: ‘wij komen pas langs als u het fout blijkt te doen’. Natuurlijk, we kunnen ook zelf een jurist inhuren, maar dat geeft nog geen garantie dat een rechter tot hetzelfde inzicht komt als zo’n jurist – die grote ruimte voor interpretatie is juist het punt.”

Een andere kwestie die Hania steekt: het ongelijke speelveld tussen Europese en Amerikaanse bedrijven. “In de VS sluit je als consument een soort contract met een bedrijf omtrent het beheer van jouw gegevens, en daarmee is privacy een civielrechterlijke zaak geworden. Amerikaanse bedrijven zijn gerechtigd om te zeggen: ‘Als iemand mij nu gegevens afstaat, mag ik daar vervolgens mee doen wat ik wil’. Ook al ontstaan er dus nieuwe toepassingsmogelijkheden voor die informatie - specifieke mogelijkheden waarvoor de verstrekker geen toestemming heeft *kunnen* geven, simpelweg omdat die mogelijkheden toen nog niet bestonden. Volgens de Europese privacywetgeving mogen wij zo niet handelen. Dat stelt ons als ondernemers op achterstand. Ik zie dat als één van de redenen dat Amerikaanse bedrijven die informatie opzuigen (Google, Facebook, etc cetera) de markt domineren ten koste van Nokia en van ons.”

Als een Amerikaans bedrijf het contract met zijn cliënt niet naleeft, kan het overigens een flinke schadeclaim verwachten - dat dan weer wel. Terwijl Europa weliswaar een strikte privacywetgeving kent, maar nauwelijks sancties oplegt. Hania: “De handhaving stelt hier weinig voor. Vandaar dat Amerikaanse bedrijven op onze markt durven te opereren. Ze ontwikkelen hun producten in de VS onder veel minder gereguleerde omstandigheden, en gokken erop dat ze hier niet op hun vingers getikt worden.”

8. Jij bent je digitale profiel

Dankzij databestanden, snelle computers en slimme software kunnen bedrijven en organisaties ons persoonlijke profiel steeds verder verfijnen en ons preciezer in subcategorieën plaatsen. De marketing wordt daar onmiskenbaar beter van. Dat wil zeggen: de kans neemt toe dat wij producten en diensten aangeboden krijgen waar we ook echt wat aan hebben. Maar van een profiel gaat ook altijd een zachte dwang uit: éét dit, léés dat, kóóp zus, stém zo – want dat past bij jouw profiel. Ongemerkt en ongewild lopen we de kans ons te gaan gedragen naar ons profiel. En dat is misschien wel een verlies. Een profiel is immers slechts een aggregaat van statistische waarheden,

een beeld samengesteld op grond van indicatoren die van tevoren bepaald zijn. Voor dat beeld van jou is nooit naar jou persoonlijk gekeken. Daarmee heeft een profiel veel weg van confectiekleding. Als je een beetje een doorsneemaat hebt, zal een profiel je aardig passen. Maar een profiel kan ook veel te ruim of veel te krap zitten. Dat zou jou probleem eigenlijk niet moeten zijn. Maar dat kan het wel worden.

Profileringstechnologie roept volgens Jan Staman, directeur van het Rathenau Instituut, al snel een wenkend perspectief op: de droom van *social engineering*. Staman: 'Door mensen in klassen te verdelen en te onderzoeken wat aanslaat bij mensen met een bepaald profiel, wordt het (..) gemakkelijker om ze zachtjes de goede richting in te duwen.'[18] Marketeers van bedrijven achterhalen zo wat effectieve reclame is. Maar ook voor bijvoorbeeld een overheid die rookverslaving wil tegengaan, zijn profielen goud waard. Het is dan immers heel handig om te weten dat rokers die al vóór hun vijftiende begonnen met roken fundamenteel anders op een maatregel reageren dan rokers die op latere leeftijd een sigaret opstaken. Zo´n overheid kan dan verschillende programma´s loslaten op rokers met een verschillend profiel. Dat werkt een stuk efficiënter.

Nu kennis en technologie steeds verfijndere profielen van groepen mensen leveren, nemen de mogelijkheden voor *social engineering* evenredig toe. Staman: 'Insiders die weten welke aanpak aanslaat bij welk profiel kunnen steeds meer 'regelaars van het mensenpark' worden, om met Peter Sloterdijk te spreken. Ze krijgen immers technieken in handen om groepen mensen slimmer te sturen.' *Social engineering* is voor Staman niet bij voorbaat taboe. Er kunnen goede redenen zijn om individuen tegen zichzelf te beschermen; denk aan arbo-regels voor bouwvakkers, of de leerplicht voor jongeren. Wel ziet Staman graag dat we publiekelijk overleggen over de vraag of het verlangen van bestuurders om rond een concreet vraagstuk bevolkingsgroepen in te delen en te sturen gerechtvaardigd is. Zijn daar goede, overtuigende redenen voor?

Daarbij is er een belangrijk verschil tussen bedrijven en overheden, een verschil dat terug te voeren is op de verschillende aard van het stilzwijgende 'contract' tussen bedrijven en consumenten, respectievelijk overheid en burgers. Het contract met een bedrijf kun je opzeggen. Dat met een staat niet. Daarom zijn er burgerrechten nodig om die staat in bedwang te houden, en is het essentieel dat de staat de mensen op haar grondgebied eerst en vooral als burgers ziet. En juist dit beeld van een mens als burger komt in de verdrukking door digitale profilering. Staman: 'In de digitale wereld verschijnen mensen snel als risicofactoren. En dat is de dood in de pot. Een staat die zijn bevolking

[18] In zijn column 'Stavast', *Flux Magazine,* mei 2012, http://www.rathenau.nl/publicaties/publicatie/flux-magazine-mei-2012.html

gaat zien als een risicofactor, houdt alleen maar schapen over, die zich mak voegen. En enkele wolven, die fel van zich afbijten. Zo'n staat is zijn burgers in ieder geval kwijt.'[19]

'ICT-innovaties' als bijvoorbeeld het Elektronisch Patiëntendossier (EPD) en het kinddossier werken in de hand dat de staat ons niet meer ziet als burger, maar als risicofactor, licht Staman toe. En de overheid kan zo'n 'risicofactor' op twee manieren corrigeren: via straf, of via hulp. "Drie rode stippen in het kinddossier betekent dat er sprake is van een riskante situatie. En dan komen er dus mensen aan de deur die het kind of de ouders dwingend hun hulp opleggen. Een dergelijke benadering past misschien binnen het Chinese harmoniemodel, dat stelt dat bestuurders en onderdanen eigenlijk allemaal in harmonie zijn en zich ook als zodanig behoren te gedragen. Maar westerlingen begrijpen zichzelf van oudsher als subjecten die hun leven zélf inhoud moeten geven. In een liberale samenleving hoort het individu voorop te staan, en zo'n individu moet zelf zijn toekomst kunnen organiseren. En dat is niet gemakkelijk; je hebt er als mens je handen vol aan."

Mensenrechten gaan uit van rechten voor het individu, en die worden in het harmoniemodel enorm geschonden. Staman: "Dat harmoniedenken is er nu in Nederland ook ingeslopen, vooral op het ministerie van Veiligheid en Justitie. De minister wil uniform gedrag afdwingen en ziet ons dus niet meer als burgers. Daar verschijnen we slechts als risicofactoren." En dat maakt Staman kwaad. Hij wil graag positie innemen, verantwoordelijkheid dragen, aangesproken worden, maar de staat doet nauwelijks meer een appèl op een dergelijk moreel agentschap van burgers. Staman: "Ik vind: iedere minister die mij indeelt in een bepaald profiel, zit aan mijn mensenrechten. Want die ziet mij niet staan als burger die zijn eigen verantwoordelijkheid neemt. Daar zit mijn pijn. Ik erken de maatschappelijke problemen wel waar de overheid voor staat, maar als de minister van Justitie in dit vocabulaire blijft hangen, dan is hij mij kwijt. Dan moet hij maar minister in China worden."

9. ICT verstoort burgerschap

In de begindagen is ICT gepresenteerd als een geweldig middel om tot actief burgerschap te komen. Burgers zouden elkaar via het internet gaan vinden, de drempel om actief bij te dragen aan het maatschappelijk debat zou veel lager komen te liggen. Die belofte is deels ook bewaarheid geworden; tal van belangengroepen organiseren zich een stuk gemakkelijker dankzij internet. Toch voelt Staman zich door ICT juist bedreigd in zijn burgerschap - met name door de profilering die ICT mogelijk maakt, en de omgangsvormen tussen burger en staat die uit die profilering voortvloeien. Deels is dit inherent aan de technologie zelf. Zoals gezegd is een profiel geen beeld van een individu, maar een min of meer verfijnd statistisch patroon dat opdoemt uit statistische gegevens uit het

[19] In zijn column 'Stavast', zie noot 17.

verleden. Een profiel heeft dus weinig boodschap aan de veranderingen en discontinuïteiten die ook een essentieel onderdeel uitmaken van het menselijk leven. Profielen bestendigen als het ware bestaand gedrag. En daar komt iets bij: omdat vooral bedrijven en dienstverleners de motor zijn achter het opstellen van profielen, bestendigen zij ons gedrag als *consument* – en niet ons gedrag als *burger*.

De ondermijning van burgerschap is volgens de Amerikaanse publicist Evgeny Morozov een onderschat effect van de digitalisering van onze identiteit. Hoor wat Morozov heeft te zeggen over Google-maps: 'In de nabije toekomst zullen de plattegronden die we te zien krijgen dynamisch worden gegenereerd en in hoge mate worden gepersonaliseerd, waarbij de plekken die onze sociale netwerkvrienden bezoeken een voorkeursbehandeling krijgen, evenals de plekken die we in onze e-mails vermelden en in de zoekmachine opzoeken. Daarentegen zullen de plekken waar we nog nooit zijn geweest – of waar we althans geen belangstelling voor hebben getoond – moeilijker te vinden zijn.'[20] Veel internettools hebben een zeer utilitair – om niet te zeggen zelfzuchtig – karakter, aldus Morozov. 'In de wereld van Google is de openbare ruimte slechts iets dat zich bevindt tussen jouw huis en het goed aangeschreven restaurant waar je graag heen wilt.'

Hoe meer we de openbare ruimte met digitale middelen ontsluiten, des te minder de openbare ruimte een plek lijkt te worden waar je andersgezinden ontmoet, kunnen we Morozov parafraseren. De openbare ruimte verschijnt hier al helemaal niet als een *polis*, een plek waar verschillende meningen en belangen botsen om vervolgens verder uitgedacht en gewogen te worden. Integendeel: op het internet verschijnt de buitenwereld op dit moment vooral als een 'echokamer' (Staman), "waar je gelijkgestemden kunt opzoeken en nooit wordt tegengesproken". Al die 'gepersonifieerde' digitale informatie maakt dat goede redenen voor burgerschap en politiek vervagen. Je wordt ingesloten door je eigen voorkeuren. Dit betekent dat je in de praktijk nauwelijks meer met verschil hoeft te leven. De openbare ruimte verdwijnt als het ware.

Dat zou ook een – paradoxale – verklaring kunnen zijn voor die opvallend lauwe belangstelling van veel mensen voor privacykwesties. Want waarom zou je je zorgen maken om je privacy als je de publieke ruimte nauwelijks ervaart? De virtuele wereld voegt zich naar jouw persoonlijke smaak, jouw persoonlijke identiteit, jouw persoonlijke keuzes. En je zaken regel je steeds meer in een virtuele wereld – ook je zaken met de overheid. De hele wereld doet zich voor als een privédomein. Je ervaart geen 'buiten' meer. Deze wilde hypothese kan ook verklaren waarom juist jongeren zo weinig gevoel voor privacy lijken te hebben. Ze zijn nog te jong om zich werkelijk als

[20] In de opiniebijlage van *NRC Handelsblad*, 1 juni 2013.

burgers op te stellen, dat wil zeggen: als deelnemers aan de publieke ruimte in de vorm van een *polis*. Jongeren voelen nog geen contrast met de buitenwereld als arena van verschil, omdat ze die arena nauwelijks betreden hebben, en omdat ze er nog geen werkelijke verantwoordelijkheid voor dragen. De suggestie die hieruit volgt: als we privacy willen redden, is het misschien vooral onze publieke ruimte die zorg, aandacht en bescherming verdient – meer nog dan onze privéruimte.

10. Heimelijkheid

'Ik heb niets te verbergen', is de reactie van sommige mensen op de onthulling dat hun handel en wandel routineus wordt gescreend door bedrijven en diensten. Toch zijn er dingen die een mens heimelijk wil doen. In je neus peuteren. Een lastig loopje op de piano oefenen. Seks hebben. Maar ook: rustig wakker worden.

Hoewel de woorden in de spreektaal vaak door elkaar gebruikt worden, betekent 'heimelijk' niet hetzelfde als 'stiekem'. Je doet dingen stiekem omdat ze moreel verwerpelijk zijn en het daglicht niet kunnen verdragen. Het is niet meer dan logisch dat orde- en veiligheidsdiensten gespitst zijn op dergelijk stiekem gedrag. Minder logisch is het dat de informatietechnologieën die deze diensten daartoe inzetten, stiekem gedrag en heimelijk gedrag automatisch op één hoop lijken te gooien. Je kunt namelijk heel goede redenen hebben om sommige, moreel onschuldige, dingen voor jezelf te houden.

'Heimelijk' is terug te voeren tot een betekenisveld dat woorden als 'heem' en 'geheim' omvat, en duidt op zaken die 'tot het huis behoren', en 'vertrouwd en voor anderen verborgen' blijven.[21] Elke cultuur kent lichamelijke handelingen waar je anderen niet mee lastig valt – bij ons bijvoorbeeld neuspeuteren en wc-bezoek. Vrijwel ieder individu voelt zich bovendien onzeker over bepaalde lichamelijke en emotionele onvolmaaktheden, die hij bij voorkeur alleen aan echte intimi toont. Zij mogen je kwetsbaar zien, omdat je op hun liefde vertrouwt. Maar privacy is er ook om te oefenen en te repeteren in besloten kring. Je wilt thuis, temidden van vrienden, een proefballonnetje kunnen oplaten. Een gedachte formuleren waarvan je de implicaties zelf ook nog niet overziet. Risico nemen met een grap die verkeerd kan vallen. Soms moeten woorden en handelingen rijpen voordat ze zinvol zijn in de openbaarheid. Als niets meer geheimzinnig kan zijn, verdwijnt de ruimte voor het experiment.

Dit geldt niet alleen voor individuele burgers. Het is ook de reden dat adviesprocessen in Nederland een tamelijk besloten karakter hebben. André Knottnerus, voormalig voorzitter van de Gezondheidsraad en huidig voorzitter van de WRR. "Zeker rond een gevoelig onderwerp wil je als

[21] Bron: *Van Dale Etymologisch woordenboek*, P.A.F. van Veen en N. van der Sijs (1997).

commissie van deskundigen een tijdje vrijuit kunnen discussiëren, zodat een advies zich kan uitkristalliseren. Een openbare tribune verlamt zo'n discussie."[22] Als iedereen op elk moment en in elk stadium van meningsvorming kan worden afgerekend op zijn of haar woorden, dan zullen juist verstandige mensen niet veel meer zeggen. Het is ook die virtuele experimentele ruimte die het begrip 'privacy' probeert te beschermen.

Privacy is te begrijpen als het recht om zelf te bepalen wie de anderen zijn voor wie wat je nu doet verborgen blijft. Positief geformuleerd: privacy geeft je de handelingsvrijheid om zelf te bepalen wat je passend vindt om aan wie te laten zien. In de woorden van internetactivist Jacob Applebaum: "Draag je kleren? Heb je gordijnen voor het raam hangen? Is dat omdat je iets te verbergen hebt? (..) De juiste vraag is niet of ik iets onder deze trui te verbergen heb, de juiste vraag luidt: is dit mijn lichaam?'"[23]

Ton Robben, wiens oma zo graag goed gekapt de telefoon opnam, is ervan overtuigd dat het een wezenlijke behoefte van mensen is om een 'binnen' en een 'buiten' te creëren. Als antropoloog ziet hij dat dit onderscheid zich altijd en overal, in elke cultuur, manifesteert - en dat is voor hem een aanwijzing dat het hier om iets essentieels gaat. "Wij mensen willen symbolische grenzen opstellen: binnen of buiten mijn lichaam, binnen of buiten mijn huis, binnen of buiten mijn gemeenschap, mijn land. En we markeren die grenzen ook fysiek - met kleren, deuren, hekken, grenzen, et cetera. De wet heeft die behoefte altijd ondersteund. Ik kan jou uitnodigen om mijn wereld te betreden, maar jou ook die toegang weigeren. Zelfs de politie heeft toestemming van de rechter nodig om jouw ruimte binnen te komen."

Die onschendbaarheid lijkt geruisloos verdwenen nu thuis de digitale communicatiekanalen volop openstaan. Robben: "Wat jij privé doet, wordt standaard en routinematig geregistreerd en opgeslagen in databestanden. Camera's volgen je, soms ook in huis - als jij Skype hebt geïnstalleerd, kan een zogenoemde *PlaceRaider* zonder dat jij het merkt een driedimensionaal beeld maken van jouw huis; Amerikaanse militairen gebruiken die techniek al om een aanval in een bepaald huis voor te bereiden." Zo kun je je nergens meer echt onbespied meer wanen. En dat kan een psychologisch ontwrichtend besef zijn. Robben: "Waar ga jij heen als je je onveilig voelt? Naar huis, misschien zelfs naar je slaapkamer, naar bed. Met andere woorden: naar je innerlijke domein. Wat nu als je weet dat je ook daar bekeken kunt worden?"

---

[22] Geciteerd in: Marjan Slob en Jan Staman: 'Beleid en het bewijsbeest: een verkenning van verwachtingen en praktijken rond evidence based policy'. Rathenau Instituut (2012). p 25.
[23] 'Anonimiteit is een Mensenrecht', *Vrij Nederland,* 16 februari 2013.

Het is maar de vraag of de nieuwe generatie geen behoefte meer heeft aan zo'n heimelijke binnenruimte, zoals weleens gesuggereerd wordt. De nonchalance waarmee veel jongeren persoonlijke informatie digitaal laten slingeren zou weleens eerder kunnen voortkomen uit gebrek aan ervaring met het 'publieke' van publieke ruimtes dan met een gebrek aan behoefte aan heimelijkheid. Paul Sasse van Ysselt, jurist op het ministerie van Binnenlandse Zaken en Koninkrijkrelaties merkt op: "Tieners laten van alles over zichzelf los op het internet, vaak wellicht zonder dat ze dat zelf in de gaten hebben. Maar tegelijk hebben ze een aller-állergeheimst dagboek dat niemand mag lezen."

Om terug te komen op de wilde hypothese: Tieners hebben behoefte aan een eigen kamer. En zoals bekend ruimen ze die zelden op. Waarom zouden ze hun spullen op internet wel opruimen? De noodzaak van opschonen komt later pas, als je werkelijk verantwoordelijkheden draagt voor je werk, je uitspraken, je kinderen. Als je een werkelijke deelnemer aan de *polis* bent geworden.

11. Bekeken worden

Als je jezelf niet aan het oog van de wereld kunt onttrekken, ben je nergens meer thuis. Dat is een afschuwelijk gevoel, vertelt Julia Behrend, die opgroeide in de DDR, in een gewone familie. De familie leefde "vanaf het moment dat ze 's morgens hun ogen opendeden met een scherp besef van wat ze buitenshuis konden zeggen (erg weinig) en wat ze binnen konden bespreken (bijna alles)."[24] Dit was de normale toestand; elke surveillancestaat dwingt haar onderdanen tot het ontwikkelen van een scherp instinct voor het verschil tussen vrienden en vreemden, binnen en buiten. Julia's situatie wordt bijzonder zodra ze een Italiaans vriendje krijgt: de Stasi begint haar actief te volgen en dringt daarmee ook haar binnenruimte binnen. Op een middag moet ze verschijnen op het bureau van een hoge Stasi-officier, die haar intimideert door haar te laten merken wat hij allemaal weet over haar intieme leven. Julia: "'Indertijd klaagde ik over andere dingen – over het feit dat ik niet kon studeren en niet kon werken. Maar als ik terugkijk, was het die totale surveillance die me het meeste heeft beschadigd. Ik *weet* hoever mensen over jouw grenzen kunnen gaan – totdat er helemaal geen privéruimte meer voor je overblijft. En dat is vreselijke kennis om mee te leven.'"[25]

De DDR wilde haar burgers actief onder de duim houden. Zo hoeft surveillancetechnologie natuurlijk niet ingezet te worden. Camera's kunnen ook met zorgzame bedoelingen worden geïnstalleerd: om zieke en kwetsbare mensen in de gaten te kunnen houden, om buspersoneel te beschermen tegen agressie, et cetera. En toch: het feit dat de buitenwereld misschien meekijkt, gaat

[24] Geciteerd in: Anna Funder, *Stasiland*, Granta (2003), p. 95
[25] Funder, op cit. p. 113.

sluipenderwijs deel uitmaken van jouw manier om hier, op deze plek, te zijn. Je gaat je ernaar voegen.

Ton Robben vertelt hoe de eigenaar van een bakkerij bij hem in de buurt camera's in de winkel liet plaatsen, omdat dit veiliger zou zijn voor het personeel. Robben: "Maar die ingreep betekende ook onherroepelijk iets voor de gesprekken die het personeel onderling kon voeren. Ze gingen op hun woorden letten. En op een gegeven moment belde de baas op: 'Wat sta jij daar als een paspop achter de toonbank!', terwijl er op dat moment geen klant in de winkel te bekennen was." De technologie maakt hier de vrije ruimte voor het personeel kleiner - onbedoeld, maar onmiskenbaar. "Foucault zou zeggen dat hier een staaltje van biomacht werd uitgeoefend", concludeert Robben.

Ook Corien Prins maakt zich zorgen over het afkalven van de privéruimte. De overheid zegt ICT in te zetten met het oog op onze veiligheid, maar: "het argument van veiligheid krijgt steeds meer onaangename trekjes. En dat terwijl veiligheid een warm woord zou moeten zijn – een woord dat staat voor geborgenheid. 'Veilig' betekent dat je een toevluchtsoord hebt en je door medemensen gedragen weet. De veiligheid die de overheid nastreeft heeft daarentegen harde kanten. De veiligheid waarin je onbespied jezelf kunt zijn, die gaat verloren."

Het is een open vraag wat de psychologische en maatschappelijke consequenties zijn van dit verlies. Wat doet het met een mens om zich niet echt meer heimelijk terug te kunnen trekken? En als jouw privéruimte steeds meer oplost in de openbaarheid, kun je dan je rol in die openbaarheid nog wel naar behoren vervullen? Kun je dan eigenlijk nog wel een burger zijn?[26]

12. Wie controleert ICT?

Of het nu komt doordat de publieke ruimte verdampt of niet, of doordat mensen zich niet realiseren wat er feitelijk op het spel staat, feit is dat het mensenrecht 'privacy' maar bij weinig mensen vurige gevoelens wakker maakt. Er zijn zeker wel organisaties die de 'digitale burgerrechten' fel verdedigen, zoals *Bits of Freedom* en de koepelorganisatie *European Digital Rights*, maar dat blijven qua omvang kleine bewegingen. Wat vooral opvalt, is de achteloosheid waarmee veel mensen privé-informatie in de publieke ruimte rondstrooien. Juist als er technologie bij te pas komt. Jan Staman: "Sommige onderwerpen bespreek je niet op een terras omdat je weet dat er allerlei mensen meeluisteren. Internet is ook een semi-publieke ruimte, maar daar zie je mensen als het ware heel

[26] Hannah Arendt zou vermoedelijk zeggen dat dit een onmogelijkheid is: actie (politieke en maatschappelijke creativiteit) krijgt vorm in de openbaarheid (de *polis*), maar moet gevoed worden door een *oikos*, een binnenruimte, waar een heel andere dynamiek tussen mensen geldt. *The Human Condition,* The University of Chicago Press, 1958.

hard roepen..” (*schreeuwt)* “..IK BEN JAN STAMAN, ZIEN JULLIE WEL WAT IK HIER AAN HET DOEN BEN!” Zo gedragen mensen zich op internet. Ze zijn zich er helemaal niet van bewust dat ze aan het schreeuwen zijn.”

Voor intelligence-and-security-wetenschapper Bob de Graaff is het de vraag waarom mensen op internet zo gemakkelijk hun gegevens afstaan. Omdat zij niet onmiddellijk met de consequenties daarvan worden geconfronteerd, vermoedt hij. De Graaff: “Je wilt nú iets, en gaat daartoe accoord met dingen waarvan je later pas de gevolgen ondervindt.” Formeel gebeurt hier misschien niets illegaals, beaamt hij. Je accepteert zelf tal van cookies. En hoe vaak klik je niet aan dat je akkoord gaat met ‘de voorwaarden’, zonder dat je die voorwaarden werkelijk serieus doorneemt? “Ik schat dat 99,9 procent van de mensen zich blind akkoord verklaart, want ze willen dóór. Terwijl er soms heel rare dingen in die voorwaarden staan; bijvoorbeeld ‘u stemt ermee in dat wij zonder u verder op de hoogte te stellen foto’s mogen maken met uw smartphone’.”

Die laksheid van consumenten geeft overheidsdiensten een argument in handen. Door de privacyregels niet al te strikt op te vatten, kunnen zij de samenleving (misschien) veiliger maken, en hun dienstverlening (misschien) efficiënter. Sommige beleidsmakers redeneren: ‘Mensen zijn bereid allerlei informatie weg te geven op sociale netwerk-sites of aan grootwinkelbedrijven. Wij doen niets anders dan Albert Heijn doet met de bonuskaart, en daar hebben mensen toch ook geen problemen mee!’” Op een bijeenkomst op het ministerie van Binnenlandse Zaken over de informatiesamenleving hoorde ik de speechschrijver van het ministerie zeggen: ‘Als je alles op straat gooit, moet je ook niet zeuren dat het op straat ligt.’[27]

Feit is dat veel mensen digitale informatie in het rond slingeren die behoorlijk privé is. Maar daaruit kun je nog niet concluderen dat hun privacy hun niet kan schelen, waarschuwt Corien Prins. “Voor niemand, zelfs niet voor echte deskundigen, is te overzien wat er gebeurt in de lagen onder de informatie die je als gebruiker invoert. Dan kun je niet van burgers verwachten dat ze precies weten wat ze op internet doen.” Simon Hania van TomTom valt haar bij: “Mijn ervaring is: gebruikers staan hun gegevens vrij gemakkelijk in vertrouwen af. Voor het hele internet geldt dat gebruikers vaak ‘ja’ zeggen tegen het verstrekken van informatie zonder dat ze zich de gevolgen daarvan realiseren. Je kunt dat onnozel noemen, maar dat vind ik te ver gaan. Wij mensen zijn ingesteld op de fysieke wereld, daar zijn we aan gewend. De virtuele wereld is nieuw en onbekend. Is het dan naïef dat je niet precies overziet op welke manier de virtuele wereld van de fysieke wereld verschilt? Gooi je dan zomaar je privacy te grabbel? Misschien. Maar je moet ook kunnen begrijpen hoe je je mensenrecht goed kunt uitoefenen.”

[27] Op 23 juni 2013 tijdens de bijeenkomst ‘de avond van de i-samenleving’ op het ministerie van BZK.

Veel van de huidige praktijken rond persoonsgegevens bewegen zich binnen de letter van de wet, omdat burgers vrijwillig en met instemming hun gegevens kenbaar maken – zowel aan de overheid als aan private organisaties. Dat doen ze veelal door de algemene voorwaarden aan te vinken. Maar je kunt je wel afvragen in hoeverre mensen nog de beheersing hebben over de mate waarin zij zich blootgeven, zegt ook Paul Sasse van Ysselt, coördinator grondrechten binnen de directie Constititionele Zaken en Wetgeving van het ministerie van Binnenlandse Zaken en Koninkrijkrelaties. Deels is die instemming fictie, want als je *niet* instemt, kun je maatschappelijk nauwelijks functioneren. Sasse van Ysselt: “Je kunt wel assertief al die voorwaarden doorlezen en zeggen: ‘jullie artikel 36 zou ik liever niet accepteren’, maar in de praktijk heb je dan geen deal, en meestal ook geen alternatief.”

Mensen die een overeenkomst sluiten met een bedrijf – een mens in de gedaante van consument dus – kunnen moeilijk peilen wat er gebeurt met de informatie die ze verstrekken. Uit het feit dat ze die informatie toch verstrekken, valt niet te concluderen dat het hen dus niet kan *schelen* wat er met hun persoonlijke informatie gebeurt. Het betekent alleen maar dat ze die drempel ondanks dat gebrek aan overzicht toch nemen.

En het betekent al helemaal niet dat de overheid dan wel de praktijken van het bedrijfsleven kan imiteren. Zodra het om betrekkingen tussen mensen en de overheid gaat, verschijnen mensen immers in hun gedaante van burger. En juist als het om persoonlijke gegevens gaat, is de staatsmacht nog altijd veel groter en gevaarlijker dan die van bedrijven. Vandaar dat extra prudentie op zijn plaats is. Bob de Graaff: “De consequenties van het feit dat de staat jouw privésfeer binnendringt zijn anders, potentieel serieuzer, dan dat een bedrijf dat doet. Het is misschien vervelend om als 55-plusser opeens advertenties te krijgen voor incontintentieluiers, maar als de staat bestanden aan elkaar gaat koppelen en jouw gangen natrekt, kan je de politie op je dak krijgen.” Bovendien is er geen garantie dat de overheid over vijftien jaar nog te vertrouwen is. Wat zal de toekomstige overheid met al die gekoppelde persoonlijke gegevens van haar burgers doen? De Graaff: “Zelf woon ik in Vlaanderen, en ik denk wel eens: stel dat België echt opdeelt en dat het Vlaams Blok een stevige vinger in de pap gaat krijgen in Vlaanderen, hoe zal mijn leven als geregistreerd ‘buitenlander’ er dan gaan uitzien?”

13. De wet aanscherpen

Ook Corien Prins vindt dat de overheid principieel anders behoort te redeneren dan private partijen. Privacy is een grondrecht, en de Grondwet is gemaakt vanuit de idee dat de overheid een bepaalde opdracht heeft, namelijk: zich niet teveel bemoeien met de burgers. “Die opdracht staat nog steeds voor de overheid.” Dus zelfs als veel burgers zich werkelijk niet om hun privacy

bekommeren en redeneren: 'ik heb niets te verbergen', dan nog heeft de overheid volgens Prins de taak om vanuit de Grondwet te handelen. Ter vergelijking: het gros van de mensen maakt geen gebruik van hun passief kiesrecht, maar daarom behoort de overheid dit recht nog wel te eerbiedigen en zelfs te stimuleren. In de Grondwet zijn immers de principes neergeslagen over het type samenleving dat we willen zijn.

Wel denkt Prins de laatste tijd na over artikel 10, het 'privacy-artikel' van de Nederlandse Grondwet.[28] Ze vindt dat dit wel heel erg als een afweerrecht is neergezet: de overheid heeft zich te onthouden van inmenging in de persoonlijke levenssfeer van haar burgers. Terwijl ze denkt dat de overheid in deze digitale wereld een meer garanderende functie zou moeten hebben. Dat vraagt om een meer actieve overheid. Prins: "Ik kijk nu iets anders tegen artikel 10 aan dan vroeger; ik zou graag zien dat de overheid vanuit het grondrecht op privacy haar verantwoordelijkheid neemt voor wat de *Googles* in deze wereld aan het doen zijn. De overheid moet er voor zorgen dat het bedrijfsleven - en natuurlijk ook de overheid zelf - zich inhouden. Zeker ook omdat de grenzen tussen overheid en private organisaties zeer diffuus zijn geworden, met al die privatiseringen en gekoppelde netwerken."

Op het ministerie van BZK blijkt jurist Paul Sasse van Ysselt volgens vergelijkbare lijnen te denken. Sasse van Ysselt: "Strikt genomen is het niet de taak van de overheid om commentaar te leveren op de afspraken die civiele partijen met elkaar maken; dan treed je juist teveel in de vrije ruimte van burgers. De contracten en voorwaarden waaronder consumenten en dienstverleners met elkaar in zee gaan, behoren zij in principe zelf uit te onderhandelen. Het concept 'instemming' of 'informed consent' is momenteel de juridische spil waar hun betrekkingen om draaien." Sasse van Ysselt vraagt zich echter wel af of dit concept in de digitale wereld nog wel voldoet. Instemming van degene die zijn gegevens afstaat blijft natuurlijk noodzakelijk, maar is die instemming voldoende om het internetverkeer goed te reguleren? "We zien hier op het ministerie wel in dat de overheid niet helemaal kan ontsnappen aan de verantwoordelijkheid om burgers te beschermen tegen bepaalde praktijken van bedrijven."

Je zou kunnen zeggen dat staatsrecht en civiel recht onder druk van de digitale revolutie naar elkaar toebuigen, stelt Sasse van Ysselt. "De drang om burgers te beschermen tegen een almachtige overheid is van oudsher een sterke pijler onder het staatsrecht. De vraag is echter waar de grootste

[28] Artikel 10 van de Nederlandse Grondwet luidt als volgt: '1. Ieder heeft, behoudens bij of krachtens de wet te stellen beperkingen, recht op eerbiediging van zijn persoonlijke levenssfeer. 2. De wet stelt regels ter bescherming van de persoonlijke levenssfeer in verband met het vastleggen en verstrekken van persoonsgegevens. 3. De wet stelt regels inzake de aanspraken van personen op kennisneming van over hen vastgelegde gegevens en van het gebruik dat daarvan wordt gemaakt, alsmede op verbetering van zodanige gegevens.' http://www.denederlandsegrondwet.nl/9353000/1/j9vvihlf299q0sr/vgrnbl6ah4zz

machtsconcentraties zich tegenwoordig bevinden. In sommige opzichten is de macht van multinationals groter dan die van de staat. We denken hier op het ministerie na over manieren waarop we het grondrecht op privacy van burgers beter zouden kunnen beschermen tegen de belangen van bedrijven."

Het team van Sasse van Ysselt bereidt ook een concrete wijziging van artikel 13 van de Grondwet voor, waarin het brief-, telefoon en telegraafgeheim is vastgelegd. Het Kabinet vindt dit grondwettelijke kader 'onvoldoende duidelijk' nu veel communicatie via elektronische kanalen plaatsvindt.[29] Sasse van Ysselt: "We moderniseren dit artikel, zodat ook e-mails en andere elektronische communicatiemethoden eronder vallen. Overigens is die bescherming in lagere wetgeving deels al uitgekristalliseerd; je zou ook kunnen zeggen dat die jurisprudentie nu naar een grondwettelijk niveau wordt getild. Het idee is om e-mails van Nederlandse burgers te beschermen tegen inzien door de overheid en door bedrijven. Of door buitenlandse mogendheden - best actueel, gezien alle oproer rond de werkwijze van de NSA. Het internationale recht beschermt die rechten overigens vaak ook al. Wij verankeren die rechten dan in ons nationale recht."

Er staan ook andere wijzigingen van het privacybeleid op stapel. Zo wordt er nu in Brussel onderhandeld over een EU-Verordening over het gebruik van persoonsgegevens door bedrijven, die straks rechtstreekse werking in de lidstaten zal hebben. In de concept-verordening staat dat consumenten het recht zouden moeten krijgen om 'vergeten' te worden; bedrijven moeten hun gegevens dus schrappen als consumenten dat willen. Ook zou de informatieplicht van bedrijven zwaarder worden: zij moeten hun klanten op een toegankelijke manier laten weten wat er gebeurt met de informatie die zij afgeven, en hoelang die informatie wordt opgeslagen.[30]

Daarnaast lobbyen de Europese privacytoezichthouders, verzameld in de zogenoemde Artikel 29-werkgroep, voor het beginsel van doelbinding.[31] Doelbinding betekent dat het gebruik van verzamelde persoonsgegevens verenigbaar moet zijn met het oorspronkelijke doel waarvoor mensen hun gegevens beschikbaar stelden. De persoonsgegevens mogen dus niet opeens voor een heel ander doel worden gebruikt – zoals in de Verenigde Staten wel mag. Sasse van Ysselt: "En dat is ook verleidelijk. Natuurlijk zou Justitie bepaalde informatie van de Belastingdienst graag willen gebruiken om fraudegevallen op te sporen, om maar een voorbeeld te noemen. Maar dat mag Justitie zonder gerede verdenking hier niet doen, omdat het ook een grondrecht is om niet mee te werken aan je

---

[29] *Brief Kabinetsvisie op e-privacy: op weg naar gerechtvaardigd vertrouwen,* ministerie van Economische Zaken, 24 mei 2013.

[30] Aldus de al genoemde *Brief Kabinetsvisie op e-privacy*, zie noot 28.

[31] Bron: website van het College Bescherming Persoonsgegevens, mededeling 18 april 2013. *http://www.cbpweb.nl/Pages/med_20130418_wp29_doelbinding_verwerking_persoonsgegevens.aspx*

eigen veroordeling – wat je indirect doet als jouw gegevens zonder jouw toestemming gekoppeld worden."

Het ministerie denkt er wel over na om de doelbinding wat te verruimen. Sasse van Ysselt: "In plaats van steeds apart toestemming te vragen om persoonlijke informatie te gebruiken voor elk nieuw doel, zouden we toestemming kunnen vragen om de informatie te gebruiken voor één specifiek domein – bijvoorbeeld de gezondheidszorg. In concreto zou je er dan mee instemmen dat de persoonsgegevens die je verstrekt ten behoeve van de zorg voor jouw gezondheid worden gedeeld en gebruikt binnen het hele domein van de gezondheidszorg. Dan hoef je niet steeds opnieuw al je gegevens op te lepelen. Dat scheelt veel bureaucratie. Maar ook hier is het zoeken naar de juiste balans tussen gemak en bescherming van de privacy."

Zowel de Europese Commissie als de Nederlandse regering stimuleren ten slotte 'privacy by design'.[32] *Privacy by design* wil zeggen dat het beschermen van persoonsgegevens van meet af aan 'ingebakken' wordt in het ontwerp van het datasysteem. De genoemde overheden stellen dit niet verplicht, maar hebben afgesproken bij voorkeur in zee te gaan met systeemontwerpers die volgens deze lijn te werk gaan. Zo hopen ze het bedrijfsleven te stimuleren om te investeren in de bescherming van persoonsgegevens. Sasse van Ysselt: "Het doel van *privacy by design* is om te vermijden dat allerlei problemen rond privacy pas blijken zodra het instrument al is ingevoerd; dus als het feitelijk te laat is. Je wilt dat - zeg - ethici en juristen vanaf het begin meedenken en al vroeg bezwaren en kritiek formuleren waarmee zij anders pas na implementatie van het instrument zouden kunnen komen."

Als ontwikkelaars al vanaf het begin rekening houden met privacy, zal informatietechnologie een minder groot privacyprobleem opleveren dan nu het geval is, denkt Sasse van Ysselt. Want er zijn volgens hem best systemen te ontwerpen die privacy goed beschermen. Sasse van Ysselt: "We zijn enigszins overrompeld door de informatierevolutie; we zijn nog lang niet uitgedacht. Maar ik geloof niet dat informatietechnologie en het respecteren van privacy *principieel* op gespannen voet met elkaar hoeven te staan."

14. Het belang van maatvoering

In zijn abstractie kan 'privacy' een groot en log woord worden, dat elke pragmatische discussie over noodzaak en maatvoering de pas afsnijdt onder verwijzing naar de grote en zuivere principes die op het spel zouden staan. Hetzelfde kan trouwens (met minstens zoveel reden) gezegd

[32] Zie de notitie *Privacybeleid* van de directie Wetgeving van het ministerie van Veiligheid en Justitie, 27 april 2011 en de in noot 28 genoemde *Brief Kabinetsvisie op e-privacy*.

worden van het begrip ‘veiligheid’. Een dergelijke manier van redeneren is maatschappelijk niet heilzaam. Je moet dan ook niet proberen om het onbehagen rond privacy met één generieke privacywetgeving weg te nemen, denkt de Rotterdamse hoogleraar ICT en sociale verandering Valerie Frissen. Een meer concrete blik kan wellicht wél een uitweg bieden uit ‘die loopgravenoorlog’ tussen privacy en veiligheid.

Het is van belang om te begrijpen dat privacy een contextueel begrip is, stelt zij. ‘In een noodsituatie – bijvoorbeeld als er in jouw omgeving een ontploffing plaatsvindt - ben je bereid veel meer gegevens over jezelf prijs te geven dan in een gewone situatie. Maar je wilt die gegevens misschien ook wel weer wissen als de dreiging voorbij is.’[33] Ook antropoloog Ton Robben memoreert dat mensen buitenstaanders altijd al toegang hebben verleend tot hun intieme omgeving, ‘bijvoorbeeld aan dokters als ze ziek zijn’. En dat anderen allerlei gegevens over jou verzamelen, is een voldongen feit. Het is volgens Corien Prins dan ook onrealistisch om te denken dat dit teruggedraaid kan worden op grond van privacy-overwegingen. Veel burgers vinden het ook helemaal niet zo erg dat overheden of bedrijven informatie over hen hebben opgeslagen, zegt zij. Daar hoeft de discussie dan ook niet te over gaan. Prins: “Belangrijk is wat er vervolgens met de gegevens gebeurt: wie maken er gebruik van, wie vult ze aan met welke informatie, hoe lang blijven ze bewaard? Dat is vrijwel oncontroleerbaar geworden. En daarmee verandert de machtsrelatie tussen de instituties en het individu, en daar moeten we het wél over hebben.”

Artikel 8 van de Europese Verklaring van de Rechten van de Mens, het privacy-artikel, legt de nadruk op proportionaliteit en subsidiariteit, en dat zijn begrippen waar je volgens Prins veel mee kunt. Prins illustreert dit met een voorbeeld: “Ik trek mijn baantjes in het Tilburgse zwembad Stappegoor. Daar kan ik alleen binnenkomen met een biometrisch pasje. Daarvoor moest ik mijn vingerafdruk achterlaten, die dan in een gedigitaliseerde vorm op mijn toegangspasje komt. Nu kan het zwembad, net als elke andere organisatie, een keuze maken tussen ‘online’ en ‘offline’ technologie. Offline technologie wil zeggen dat ik bij aanvraag van het pasje naam en geboortedatum afgeef en mijn vingerafdruk achterlaat. De scan van mijn vingerafdruk komt vervolgens op het pasje, maar de achterliggende gegevens hoeven niet óók op het pasje te staan. In dat geval kiest het zwembad voor ‘offline’ technologie. De man de ingang ziet dat ik geautoriseerd ben op binnen te komen als ik op zondagochtend ga zwemmen, maar hij ziet niet dat het pasje hoort bij Corien Prins. Bij ‘online’ technologie wordt dat wél op het pasje gezet, en verschijnen mijn gegevens in het computersysteem. Die man ziet dus iedere keer wie ik ben. Is dat nodig? Dat hangt van het doel van

[33] Uit Frissens mond opgetekend tijdens de Avond van de i-samenleving, Ministerie van BZK, 23 juni 2013.

het pasje af. Het zwembad wil via zo'n pasje ellendelingen buiten de deur houden. En dat kan net zo goed met 'offline' als met 'online' technologie."

De Europese Verklaring zegt in feite, aldus Prins, dat je moet kijken naar het doel van een maatregel en vervolgens moet kiezen voor het middel dat het minst inbreuk doet op privacy. "En dat is in dit geval de 'offline' methode, zodat die man niet kan denken: 'Goh, wat is Corien Prins vroeg, ze komt anders altijd om 11 uur!', of: 'Hé, ze neemt nu een andere man mee'. Vaak kiezen organisaties voor de meest uitgebreide maatregel en beseffen ze niet eens dat het ook anders kan. En dat moet – en kan – veranderen." Als het aan Prins ligt, bekijken we in elk concreet geval waarin instanties persoonsgegevens beheren, of de middelen in evenwicht zijn met het doel, ofwel: of de maatvoering passend is. Prins: "Ik ben niet tegen het inzetten van technologie met het oog op veiligheid. Maar ik ben wel tegen de introductie van systemen zonder een discussie over de maatvoering."

Voor Jan Staman is de cruciale vraag wie eigenlijk baat heeft bij digitale bestanden met persoonsgegevens. Neem het Elektronisch Patiëntendossier. Dat EPD slaat de medische dossiers van patiënten centraal op, met als doel dat zorgverleners snel gegevens over patiënten en hun medicijngebruik kunnen uitwisselen. Wat Staman betreft dreigt hier iets mis te gaan met de maatvoering. Staman: "Je zou je medische gegevens ook op een USB-stick kunnen zetten, die je meeneemt als je naar de dokter of de apotheek gaat. Maar de medische sector is als de dood voor zo'n oplossing, want dan zijn ze de macht over je kwijt. Met zo'n stickie kun je namelijk gemakkelijk naar een andere apotheek of cardioloog, en nu maakt de arts uit waar je heen gaat. Als je een kopie van je eigen dossier vraagt, vinden veel medici dat nu al een vertrouwensbreuk." Dat noopt Staman tot een oneliner over systemen als het EPD: "Ik ga er onmiddellijk in als Willem-Alexander er ook in gaat. En dan kun je nog heel lang wachten."

15. Autonomie krijgen over je gegevens

Bob de Graaff zou waarschijnlijk wel voelen voor zo'n stickie met persoonlijke medische gegevens. Het past in ieder geval in de lijn van zijn pleidooi: zorg dat burgers zélf hun gegevens kunnen beheren. Dan krijgen burgers de autonomie terug over hoe ze digitaal verschijnen. En zo erken je dat een mens geen dataset is, geen 'piece of information', maar een subject. De Graaff: "Ik pleit voor een soort gegevensrecht. Ik stel me een soort kluis voor op internet waarin jij al je persoonlijke gegevens opbergt – je testament, je medische gegevens, wat al niet. Dan heb je meer controle over je gegevens en zie je ook zelf waar de fouten in de registratie zitten."

Ook volgens Valerie Frissen zou de stelregel moeten zijn dat de data van de burger zijn en blijven. Als dat goed geregeld is, wordt het strikt afschermen van gegevens volgens haar zelfs van

secundair belang. Frissen: 'Belangrijker is dat je zicht krijgt op wie wat doet met jouw gegevens, en wanneer. En dat je die persoon daarop kunt aanspreken. Het zou normaal moeten worden dat mensen of instanties verantwoording afleggen over wat ze met jouw gegevens doen.'[34] Paul Sasse van Ysselt van het ministerie van BZK voelt wel wat voor de idee dat burgers meer autonomie krijgen over hun gegevens. Het ministerie discussieert intern over 'ontkoppelen' (naar analogie met 'ontvrienden'), wat burgers de mogelijkheid zou geven om eenmaal verstrekte informatie weer terug te trekken. Sasse van Ysselt: "Dat is nu heel moeilijk; je kunt je haast niet uitschrijven uit een systeem." Dit idee is nog niet geconcretiseerd in een traject. Maar Sasse van Ysselt denkt dat via dergelijke concrete aanpassingen privacy ook in de ditigale wereld te beschermen is.

In de huidige digitale wereld zal het niet meer lukken om persoonlijke gegevens volledig af te schermen. Maar dat is wellicht ook niet wat privacy van oudsher beoogt. Zodra je je in openbare sferen beweegt, ben je zichtbaar. Of je jezelf nu zichtbaar maakt op de klassieke manier - door in een zaaltje, vanaf een zeepkist, in het parlement, tijdens een demonstratie, je stem te roeren - of door vanachter je bureau tussen de vier muren van je huis je opinie te *posten* op het internet. Met zichtbaarheid komt verantwoordelijkheid. En bij verantwoordelijkheid hoort dat je te identificeren bent. Dat geldt niet alleen voor de betrekkingen tussen burger en staat. Ook mensen die op het punt staan een deal met elkaar te sluiten, willen natuurlijk weten met wie ze van doen hebben - en dus waar ze verhaal kunnen halen als het product of de dienst tegenvalt, of als betaling uitblijft. Dat is allemaal eigenlijk zo logisch dat het vreemd is dat de discussie over privacy zich vaak op die traceerbaarheid lijkt toe te spitsen. Net zoals het vreemd is dat mensen op internet kunnen schelden en dreigen zonder daarop aangeproken te kunnen worden.

Maar een mens moet wél autonomie kunnen houden over zijn identiteit. Dat houdt in dat hij weet hoe zijn digitale ideniteit verschijnt en die kan aanpassen. En hij moet zich ook terug kunnen trekken uit die publieke ruimte. Het recht om bepaalde bestanden te wissen zou aan die behoefte tegemoetkomen.

En dan is er nog die psychologische kant: soms wil je onzichtbaar zijn voor de ogen van de buitenwereld. Geen verantwoording hoeven afleggen. Heim zijn. Om weer te voelen wie die persoon eigenlijk is die geregeld de publieke ruimte betreedt. Je onbespied kunnen weten in je privéwereld is iets om te koesteren en te waarderen. Het lijkt erop dat we het belang van heimelijkheid opnieuw aan het uitvinden zijn in de digitale nieuwe wereld.

[34] Aldus Frissen tijdens een workshop op het ministerie van BZK, zie noot 33.

Kader: Geldende wetten over privacy

UVRM

Artikel 12 van de Universele Verklaring van de Rechten van de Mens luidt:

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

Nederlandse Grondwet

De Nederlandse Grondwet (versie 2008) kent drie artikelen die van belang zijn voor de bescherming van privacy:

Artikel 10 (privacy)

1. Ieder heeft, behoudens bij of krachtens de wet te stellen beperkingen, recht op eerbiediging van zijn persoonlijke levenssfeer.

2. De wet stelt regels ter bescherming van de persoonlijke levenssfeer in verband met het vastleggen en verstrekken van persoonsgegevens.

3. De wet stelt regels inzake de aanspraken van personen op kennisneming van over hen vastgelegde gegevens en van het gebruik dat daarvan wordt gemaakt, alsmede op verbetering van zodanige gegevens.

Artikel 12 (huisvrede)

1. Het binnentreden in een woning zonder toestemming van de bewoner is alleen geoorloofd in de gevallen bij of krachtens de wet bepaald, door hen die daartoe bij of krachtens de wet zijn aangewezen.

2. Voor het binnentreden overeenkomstig het eerste lid zijn voorafgaande legitimatie en mededeling van het doel van het binnentreden vereist, behoudens bij de wet gestelde uitzonderingen.

3. Aan de bewoner wordt zo spoedig mogelijk een schriftelijk verslag van het binnentreden verstrekt. Indien het binnentreden in het belang van de nationale veiligheid of dat van de strafvordering heeft plaatsgevonden, kan volgens bij de wet te stellen regels de verstrekking van het verslag worden uitgesteld. In de bij de wet te bepalen gevallen kan de verstrekking achterwege worden gelaten, indien het belang van de nationale veiligheid zich tegen verstrekking blijvend verzet.

Artikel 13 (briefgeheim)

1. Het briefgeheim is onschendbaar, behalve, in de gevallen bij de wet bepaald, op last van de rechter.

2. Het telefoon- en telegraafgeheim is onschendbaar, behalve, in de gevallen bij de wet bepaald, door of met machtiging van hen die daartoe bij de wet zijn aangewezen.

EVRM

Het Europees Verdrag voor de Rechten van de Mens kent artikel 8, het zogenoemde *Recht op eerbiediging van privéleven, familie- en gezinsleven*.

1. Een ieder heeft recht op respect voor zijn privéleven, zijn familie- en gezinsleven, zijn woning en zijn correspondentie.

2. Geen inmenging van enig openbaar gezag is toegestaan in de uitoefening van dit recht, dan voor zover bij de wet is voorzien en in een democratische samenleving noodzakelijk is in het belang van de nationale veiligheid, de openbare veiligheid of het economisch welzijn van het land, het voorkomen van wanordelijkheden en strafbare feiten, de bescherming van de gezondheid of de goede zeden of voor de bescherming van de rechten en vrijheden van anderen.

Handvest van de Grondrechten van de Europese Unie

* Het recht op bescherming van persoonsgegevens wordt op gelijkwaardige wijze beschermd door artikel 8 van het Handvest van de Grondrechten van de Europese Unie (2000). Dat artikel luidt als volgt:

1.Eenieder heeft recht op bescherming van de hem betreffende persoonsgegevens.

2. Deze gegevens moeten eerlijk worden verwerkt, voor bepaalde doeleinden en met toestemming van de betrokkene of op basis van een andere gerechtvaardigde grondslag waarin de wet voorziet. Eenieder heeft recht op toegang tot de over hem verzamelde gegevens en op rectificatie daarvan.
3. Een onafhankelijke autoriteit ziet toe op de naleving van deze regels.

Raad van Europa

In 1981 heeft de Raad van Europa het *Verdrag tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens* (Verdrag nummer 108) vastgesteld. Dit verdrag wordt momenteel gemoderniseerd.

De in en voor Nederland vigerende wetten beschermen de privacy dus uitdrukkelijk. De pijn zit elders. Allereerst in de handhaving. Maar ook in de kennelijke verlegenheid met digitaal dataverkeer, waardoor de grenzen tussen privéruimte en buitenwereld dermate diffuus zijn geworden dat de wetgever er (nog) niet goed raad mee weet. Wat telt in deze omstandigheden als huisvredebreuk?