Samenvatting

Dit boek verschaft een kijkje achter de schermen van moderne ICT. Het onthult hoe het gebruik van computers ons leven niet alleen gemakkelijker en veiliger maakt, maar ook nieuwe risico's introduceert, vooral voor onze privacy maar ook voor onze persoonlijke veiligheid. Het toenemend gebruik van ICT voor identiteitscontrole, gegevenscontrole, centrale opslag van persoonsgegevens en profilering mag bedoeld zijn ter vergroting van de publieke veiligheid, maar heeft ook negatieve gevolgen zoals afgedwongen transparantie, vervreemding en identiteitsfraude, en op den duur mogelijk zelfs ook conformisme en volgzaamheid uit angst voor een *bad profile*, waardoor verdere uitsluiting en isolement volgt.

Tegenover dit sombere beeld wordt onderzocht hoe een menselijke maat in ICT gerealiseerd zou kunnen worden via moderne technieken, met aandacht voor differentiatie (in plaats van uniformisering) en kleinschaligheid. Wezenlijk daarbij is dat persoonlijke informatie zoveel mogelijk onder directe controle staat van de individuen die het betreft, bijvoorbeeld via decentrale opgeslag bij mensen zelf. Informatie is macht, en verdeling van informatie en macht is noodzakelijk om op de langere termijn individuele autonomie te kunnen waarborgen. Daarbij is het nodig dat individuen beter bekend zijn, en om kunnen en willen gaan, met moderne technieken. Bij dit alles dienen we ons scherp bewust te zijn van de consequenties van de keuzes die we nu maken om wel of niet zulke privacyvriendelijke technieken te ontwikkelen en in te zetten. Belangrijke aanbevelingen daarbij zijn: (1) pas registratie en monitoring van het gedrag van burgers alleen selectief (en niet breed en ongericht) toe, en (2) geef mensen individuele zeggenschap en eigen controlemogelijkheden in identiteitsvaststellingen en gegevensopslag.

De Menselijke Maat in ICT

Bart Jacobs

B.Jacobs@cs.ru.nl http://www.cs.ru.nl/B.Jacobs

Versie 1.0, Januari 2007

ISBN 978-90-9021619-5

Voorwoord

De menselijke maat in ICT?! Dit klinkt vreemd en tegenstrijdig. ICT heeft de naam juist geen oog te hebben voor de menselijke maat. ICT werkt uniformiserend, en mogelijk zelfs dehumaniserend. ICT leidt tot grote databanken waar we als nummers in zitten, waardoor we allemaal op dezelfde manier behandeld worden, en wel op een zodanige beperkte wijze die alleen door de computer begrepen wordt. Het antwoord "het kan alleen zo volgens de computer" op een enigszins afwijkend verzoek kennen de meesten van ons helaas maar al te goed.

Toch hoeft dit niet noodzakelijk zo te zijn. De eerste generaties computers waren inderdaad sterk centralistisch georganiseerd. Maar tegenwoordig zijn computers (en geheugens en verbindingen) zo goedkoop dat velen van ons inmiddels allerlei 'persoonlijke' computers met ons meedragen in de vorm van GSMs, organisers, mp3-spelers, spelcomputers, GPS-ontvangers of laptops. Deze 'democratisering' van apparaten heeft geen gelijke tred gehouden met het beheer van gegevens en identiteiten dat nog steeds veel 'centralistische' en 'autoritaire' trekjes kent. Dit boekje wil een aanzet geven tot een verdieping van de discussie over de huidige en toekomstige inrichting van onze ICT-infrastructuur, met oog voor de maatschappelijke aspecten. De nadruk ligt daarbij op de positie van het individu en op de wens om ICT vóór het individu te laten werken in plaats van ertegen. Onderwerpen als veiligheid en privacy—en het spanningsveld daartussen—spelen noodzakelijkerwijs een belangrijke rol.

Waarom dit boek, en voor wie?

Aan de universiteit doe ik vooral technisch werk op het gebied van computerbeveiliging. Daarbij gaat het om het reguleren van toegang tot gevoelige digitale gegevens, zoals bijvoorbeeld tot commerciële of militaire geheimen maar ook tot persoonlijke medische of financiële gegevens. Belangrijke vragen zijn: wie heb je tegenover je, hoe weet je dat zeker, wat mag die persoon of computer doen, hoe controleer je dat, en wat doe je als het fout gaat? Een wezenlijk onderdeel van het vak computerbeveiliging is een skeptische, ondermijnende houding: het gaat niet primair om de leuke dingen die je met computers kunt doen (de functionaliteit), maar meer om de nare, onbedoelde dingen en om wat er dus allemaal fout kan gaan (de risico's). Daarbij wordt met de blik van een hacker naar computersystemen gekeken. Deze kwajongensachtige houding komt in het vervolg meermaals naar voren.

Dit onderdeel ‘beveiliging’ binnen de informatica heeft nadrukkelijk maatschappelijke relevantie: ik schat dat het in meer dan de helft van de keren dat computergerelateerde onderwerpen in de pers aan bod komen gaat over beveiligingsissues, zoals virussen, inbraken, spyware, biometrische paspoorten, elektronisch stemmen, verlies van gegevens via memory sticks of complete computers, opslag verkeersgegevens, privacy, enzovoort.

In mijn contacten buiten de universiteit, bijvoorbeeld met journalisten en beleidsmakers, ervaar ik steeds dat het haast ondoenlijk is om technische en daarmee samenhangende maatschappelijke ontwikkelingen in een paar zinnen te plaatsen[1]. Met dit boek wil ik daar met meer dan een paar zinnen een uitgebreidere poging toe wagen. Meer inzicht in deze ontwikkelingen is belangrijk omdat de keuzes die gemaakt worden met betrekking tot de organisatie van ICT-infrastructuur direct invloed hebben op onze onderlinge omgang. Informatie is macht, en dus zijn de keuzes met betrekking tot opslag en toegang tot informatie nadrukkelijk ook politiek van aard. Informatici zijn niet langer alleen de architecten van de digitale wereld, maar ook van de sociale wereld.

De doelgroep voor dit boek is dus breed, en omvat iedereen die op een of andere manier betrokken is bij, of geïnteresseerd is in, het gebruik en de organisatie van ICT in onze samenleving. Er wordt geen specifieke technische kennis verondersteld. De uiteenzettingen en discussies zijn over het algemeen gericht op de *big picture* en zijn meestal niet technisch van aard. Wel is het op enig moment nodig een aantal elementaire zaken over digitale versleuteling en ondertekening op een rijtje te zetten. Een zekere affiniteit met ICT in algemene zin is dus prettig.

Dit boek is nadrukkelijk geen wetenschappelijke studie voor vakgenoten. Een afstandelijke wetenschappelijke stijl met veel verwijzingen naar het werk van collega’s wordt dan ook niet gehanteerd. Integendeel, de stijl en voorbeelden zijn af en toe persoonlijk of luchtig, waarbij de eigen betrokkenheid en voorkeuren soms expliciet aanwezig zijn. Er staan ook geen echt nieuwe, wetenschappelijk originele, theorieën in. Veel van de ideeën komen in een of andere vorm al voor in de vakliteratuur over dit onderwerp[2]. Maar die gedachten zijn misschien onvoldoende uit de wiskundige wereld losgekomen en doorgedrongen tot bijvoorbeeld systeemontwerpers, journalisten, bestuurskundigen, politici, beleidsmakers, en het algemene publiek. Ondanks dit ontbreken van verwijzingen staat aan het eind wel een kort lijstje boeken als handreiking aan de lezer die zich verder in één of meer onderwerpen wil verdiepen.

Met het schrijven van dit boek begeef ik me dus nadrukkelijk buiten de enge paden van mijn strikt wetenschappelijke werk en zoek ik de breedte en schuw ik de vergezichten niet. Dat maakt me vanzelfsprekend kwetsbaar voor detailkritiek op terreinen die niet de mijne zijn en voor verwijten dat ik me maar beter bij mijn leest kan houden. Dit is inderdaad een risico, zeker omdat Nederland helaas geen grote traditie

[1] Daarbij speelt een rol dat in deze kringen weinig technisch onderlegde mensen werken. Het zogenaamde beta tekort heeft ook hier invloed.

[2] Veel is bijvoorbeeld al te vinden in het werk van cryptografen als David Chaum uit het eind van de jaren tachtig.

kent van (exacte) wetenschappers die de brede kwast in plaats van het fijne penseel hanteren, zoals bijvoorbeeld wel gebeurt in Angelsaksische overzichtswerken als Bill Bryson’s *A Short History of Nearly Everything* en Jared Diamond’s *Guns, Germs and Steel*—waarbij ik overigens dit bescheiden boekje op geen enkele manier zou willen vergelijken met deze twee grootse boekwerken.

Waarom menselijke maat nodig?

De laatste jaren worden wij allen steeds nadrukkelijker omringd door computers die van alles van ons doen en laten registreren en vastleggen. De administraties van scholen, ziekenhuizen, bibliotheken, overheden en bedrijven worden (of zijn al) gedigitaliseerd en soms onderling gekoppeld, waardoor allerlei meer of minder gevoelige gegevens makkelijker en langer toegankelijk zijn. Dat heeft voor en nadelen. Tegelijkertijd is openbare veiligheid een belangrijk onderwerp geworden, niet alleen door de zorgen over gewone misdaad, maar vooral ook over zware criminaliteit en terrorisme. De roep om veiligheid vertaalt zich snel in sterkere controle waardoor nog meer over ons geregistreerd en vastgelegd wordt. Privacy wordt daarbij snel als hinderlijk gezien.

In het licht van deze ontwikkelingen kan men zich zorgen gaan maken om *Big Brother*[3], om afglijden tot een politiestaat, om totalitaire machtsuitoefening, of, meer in het algemeen, om verlies van persoonlijke vrijheid en autonomie. Ik ga er vooralsnog optimistisch van uit dat individuele vrijheid voorlopig niet in het geding is, maar dan wel ingeperkt binnen een steeds enger kader waarin vaker en indringender gecontroleerd wordt of we ons wel aan de regels houden. Steeds mee van onze daden zijn zichtbaar en controleerbaar, waardoor steeds vaker om verantwoording gevraagd kan worden—hier en nu reeds, in het ondermaanse, en niet pas ginder in het hiernamaals. Computers spelen daarbij een cruciale rol. Er komt zo steeds minder ruimte om “lekker stout” (naar Annie M.G. Schmidt) te zijn. Ook worden we sterker afhankelijk van autoriteiten en bedrijven die de regels stellen en controleren. Voor een deel kiezen we er natuurlijk ook zelf voor ons om meer te laten leiden en controleren door computers en minder zelf na te denken, bijvoorbeeld in het gebruik van navigatiesoftware en van spellingscheckers. Privacy staat inderdaad niet alleen onder druk van ‘veiligheid’ maar ook van ‘gemak’.

Samenhangend hiermee wordt de volledige terloorgang van privacy voorzien. Hedendaagse discussies over privacy vervallen inderdaad vaak in verzuchtingen dat het allemaal al lang verloren is—een treffend voorbeeld is de uitspraak van Scott McNealy, grote baas van het Amerikaanse computerbedrijf SUN in 1999: *You have zero privacy anyway – get over it!*—of dat de huidige focus op terrorismebestrijding geen ruimte laat voor een redelijke discussie. Een positieve boodschap over privacy gebaseerd op technische mogelijkheden wordt niet veel gehoord. Toch zullen we het juist van bewust gekozen technische maatregelen moeten hebben als we op de langere termijn enige vorm van privacy overeind willen houden. Dit inzicht, dat overigens

[3] Ook wel bekend als: Broer Koekeloer.

volstrekt niet nieuw is, ligt ten grondslag aan dit boekje. Nu worden er allerlei keuzes gemaakt met betrekking tot de organisatie van de ICT-infrastructuur (rekening rijden, OV-chipkaart, biometrisch paspoort, Burger Service Nummer, opslag verkeersgegevens) die om een zorgvuldige afweging vragen, om te voorkomen dat we over een jaar of tien, twintig hoofdschuddend tegen elkaar zeggen: hoe hebben we het ooit zover kunnen laten komen?

Een belangrijk onderdeel van die afwegingen is hoe we omgaan met identiteiten en persoonsgegevens. Hier komt de 'menselijke maat' naar boven. Het grote probleem is dat we in toenemende mate omringd worden door allerlei computersystemen die onze identiteit willen of moeten kennen zonder dat wij er enige controle over hebben wat er vervolgens met onze persoonsgegevens gedaan wordt. Gevolgen daarvan zijn (1) een gevoel van vervreemding, door onzekerheid over de eigen privacy en het soms vernederende karakter van controles[4], (2) een afname van het vertrouwen in deze ICT-infrastructuur, en (3) niet-efficiënt gebruik van deze middelen (denk aan betalingen via internet). De 'menselijke maat' oplossing waar hier op aangestuurd wordt omvat een radicale decentralisatie van velerlei structuren en processen zodat de mens (als gebruiker) zelf centraal komt te staan in de automatisering, en niet de ICT-processen of proceseigenaren. Uiteindelijk leidt dit, in het laatste hoofdstuk (21), tot een voorstel voor een *trusted personal digital assistant* (TPDA): een persoonlijke handcomputer die de sluis vormt tussen jou en de ICT-systemen die jou omringen en de kluis waarmee je allerlei persoonsgegevens zelf kunt beheren. Dit apparaatje is aan jou persoonlijk gekoppeld via biometrie (met onboard verificatie) en moet niet te vervalsen zijn. Het vormt jouw beheersmiddel voor jouw persoonlijke gegevens, identiteiten en gebruiksbeslissingen (*policies*). Om vertrouwen in zulke TPDAs te hebben is een zo open mogelijk ontwerp en realisatie vereist, met open standaarden en open source software, zodat iedereen in principe kan (laten) controleren hoe deze 'kluis en sluis' werkt en wat hij doet.

Pas nu computerhardware zo klein en goedkoop geworden is behoort het tot de mogelijkheden om de ideeën te gaan realiseren die in feite al langere tijd rondzweven in onderzoeksgemeenschappen. Dit boekje beoogt deze ideeën voor een breder publiek uiteen te zetten, met het uiteindelijke doel tot realisatie ervan te komen. Nederland heeft een lange en gewaardeerde traditie op het gebied van individualisme waarin zeggenschap over anderen eigenlijk alleen in functionele zin geaccepteerd wordt. Daarom zou het niet vreemd zijn wanneer juist wij bij de uitvoering van de hier beschreven ideeën een vooraanstaande rol zouden spelen. De politieke wind van de laatste jaren is erg gericht op individuele verantwoordelijkheid en keuzevrijheid voor de burger/consument. In de sfeer van het beheer van gegevens is deze wind echter nog niet doorgedrongen. De 'klant' mag wel kiezen maar niks beheren en wordt ondertussen als dom nummer door het ene na het andere controlepoortje gejaagd. Op de achtergrond speelt bij deze ontwikkelingen een politieke machtsvraag. Krijgen grote organisaties

[4]De gedwongen afgifte van vingerafdrukken bij binnenkomst in de Verenigde Staten geeft bijvoorbeeld snel het onwelkome gevoel als crimineel behandeld te worden.

zoals overheden en grote bedrijven nog meer macht over individuen, of kiezen we er voor (nu veel infrastructuur nog in opbouw is) om informatie en macht te decentraliseren om een redelijk machtsevenwicht te behouden?

Identiteitsfraude

Samen met de hierboven genoemde voortschrijdende vastlegging van (persoons)gegevens zien we een nieuwe vorm van fraude ontstaan, namelijk zogenaamde identiteitsfraude. Daarbij worden de negatieve gevolgen van de ontwikkelingen een concrete zorg voor individuen. Een onbenullig voorbeeld van zulke fraude is om bij een congres met het naamkaartje van iemand anders rond te gaan lopen. Zoiets kan ernstiger gevolgen hebben in een kerncentrale. Het komt steeds vaker voor dat een kwaadwillende bewust de identiteit van iemand anders aanneemt om bijvoorbeeld betalingen via het web te doen, waardoor de ander met de problemen zit. Vaak is die ander trouwens niet de enige met problemen, zoals bijvoorbeeld bij de kerncentrale. Identiteitsfraude in elektronische vorm is een onderdeel van allerlei vormen van *cybercrime*, waarin inmiddels meer geld schijnt om te gaan dan in de drugshandel.

In de context van identiteitsfraude zijn wezenlijke vragen: hoe weten we eigenlijk zeker met wie we te doen hebben? En: hoe zeker moeten we dat überhaupt weten? Een dilemma is of het voor het bestrijden van identiteitsfraude nodig is om identiteiten beter bij te houden, of juist niet: wanneer transacties 'identiteitsarm' zijn kunnen er ook geen identiteiten bij gecompromiteerd raken voor misbruik. De standaardreflex 'vergroot de identificeerbaarheid' wordt hier genuanceerd en besproken in het licht van bijbehorende risico's. Als alternatief wordt 'verklein de identificeerbaarheid' gepresenteerd, bijvoorbeeld via attributen en pseudoniemen.

Het is vervelend maar we zullen moeten leren ons beter bewust te zijn van identiteiten, bijvoorbeeld wanneer we iemand anders op het web (in cyberspace) tegenkomen, en ons vaker af te vragen: in welke mate weet ik eigenlijk zeker met wie ik hier te doen heb, en in welke mate is dat echt nodig? Maar ook andersom is het verstandig je bij elk (elektronisch) contact af te vragen: wat weet de andere partij eigenlijk van mij, en in hoeverre zou van die kennis misbruik gemaakt kunnen worden? Vaak blijkt dat allerlei transactie mogelijk zijn op basis van attributen (eigenschappen) of pseudoniemen zonder dat daar een persoonlijke identiteit aan te pas hoeft te komen.

Controle en profilering

In samenhang met de genoemde afname van privacy en toename van identiteitsfraude is er nog een andere ontwikkeling die een thema vormt in dit boek, namelijk profilering. Het is een feit dat van ons allen steeds meer digitale sporen geregistreerd en opgeslagen worden. Bewustwording van alle moderne monitoring van individueel gedrag kan leiden tot zelfcensuur of tot schaamteloosheid. Misschien is deze laatste houding wel het beste voor de eigen geestelijke rust en welbevinden, maar ik verwacht niet dat veel mensen die staat van onthechting daadwerkelijk bereiken. Zelfcensuur

heeft positieve en negatieve kanten. Er is niks mis mee wanneer zelfcensuur een inidividu ertoe brengt zich aan de wet te houden. Maar zelfcensuur die de eigen individuele ontplooing (binnen de wet) in de weg staat zien we meestal toch als negatief. Zulke censuur kan individuen hinderen in de eigen ontwikkeling en creativiteit, waar we uiteindelijke collectief nadelen van kunnen ondervinden: er worden bijvoorbeeld minder mooie boeken geschreven of minder innovatieve technieken ontwikkeld, leidend tot economische achterstand of zelfs schade.

Een recente trend is om de opgeslagen gegevens te gebruiken om profielen van mensen te maken, bijvoorbeeld als 'mogelijke terrorist, op een schaal van 1 tot 100'. Zulke profielen vormen dan de basis voor zwarte lijsten, (*black lists*) zoals in de luchtvaart al gebruikelijk is. Profilering in de commerciële wereld is natuurlijk al wijd verbreid. Zo is het gebruikelijk bij bezoek van de site van een online boekenwinkel zoals *Amazon* een aanbieding te krijgen op basis van eerder aankoop (of klik) gedrag—en natuurlijk ook op basis van de (stagnerende) voorraden van de boekwinkel. Dit soort pogingen tot gerichte aanbiedingen op basis van profielen zijn relatief onschuldig. Maar steeds vaker gaat het ook om uitsluiting, waarbij iemand de toegang geweigerd kan worden—tot een gebouw, een vlucht, of dienst, zoals een hypotheek of verzekering—op basis van een "virtuele identiteit" die construeerd is uit gegevens in databanken. Deze ontwikkelingen kunnen problematisch zijn bijvoorbeeld wanneer de gegevens onjuist zijn of wanneer de gehanteerde criteria dubieus (en niet expliciet) zijn. Deze nadruk op gebruik van ICT voor controle en profilering leidt sluipenderwijs tot een samenleving die we waarschijnlijk niet willen, waarin voor individuele afwijking van meer of minder expliciete normen geen plaats meer is. Willen we met criteria als conformisme en volgzaamheid de strijd aangaan met India en China? Ook hier geldt dat de kracht (ook economisch) van onze samenleving juist ligt in het open karakter ervan, met ruimte voor individuele autonomie, ontplooing, creativiteit en afwijking.

De huidige trend van omgaan met veiligheids- en identiteits-issues leidt, enigszins gecharcheerd, tot een 'veiligheids-communisme' waarbij de vermeende veiligheidsbelangen van het collectief de individuele veiligheidsbelangen en daarvoor noodzakelijke privacy overstemmen. Individuen zijn nummers, met een chip in hun pas of nek, en worden uniform behandeld en continue gecontroleeerd. Dit is vergelijkbaar met economisch communisme dat ook de (economische) belangen van het collectief boven die van het individue stelt, en daardoor op de langere termijn geen levensvatbare strategie bleek te bieden.

Bij deze ontwikkelingen is het goed steeds vragen te stellen als: is het effectief, wat zijn de gevolgen, willen we dit, en wat zijn de risico's voor individuen? In dit boekje zal de nadruk op het laatste punt liggen. We krijgen te maken met nieuwe persoonlijke risico's die samenhangen met de steeds alomvattender ICT-infrastructuur, zoals bewust of onbewust lekken van gevoelige persoonsgegevens uit grote databanken, identiteitsfraude, en uitsluiting op basis van profilering. Deze risico's kunnen in gecombineerde en daarmee versterkte vorm optreden: wanneer slordig met mijn gegevens omgegaan wordt kan iemand anders zich daarmee als mij voordoen en zich misdragen waardoor

ik een *bad profile* krijg en vervolgens zelf overal buitengesloten word. Deze risico's zijn niet slechts een persoonlijk maar ook een maatschappelijk probleem, vanwege de resulterende ontsporing van het maatschappelijke verkeer.

De noodzaak onze maatschappij te beschermen tegen interne en externe dreigingen maakt een zekere mate van monitoring en controle noodzakelijk. Hier wordt er echter voor gepleit deze monitoring en controle vooral selectief te gebruiken, voor de *bad guys* en niet voor de *good guys*. Dit selectieve gebruik kan op twee manieren: vooraf op basis van een redelijk vermoeden, en achteraf als straf. Ook hier is een expliciete politieke keuze gewenst: moet de overheid werkelijk al haar onderdanen wantrouwend benaderen en tot transparantie dwingen 'voor het geval dat', of moet de overheid haar burgers in principe met vertrouwen tegemoet treden. In het tweede geval moeten de burgers ook de organisatorische en technische ruimte krijgen om hun eigen identiteiten en gegevens te beheren, 'tenzij'. Deze laatste keuze getuigt van meer respect voor de individuele autonomie.

Traditioneel wordt vrijheid door filosofen niet gezien in passieve termen (zappen op de bank, consumeren zoals aangestuurd door reclames) maar als iets dat mensen actief vorm moeten geven in het zelf overstijgen van dierlijke verlangens en reflexen. Met de toenemende automatisering wordt ook autonomie iets dat steeds actiever vormgegeven dient te worden, omdat zoveel handige en veilige gadgets en systemen de zaken van ons overnemen. De grote vraag wordt dan of we hierdoor werkelijk geholpen worden en ons op de wezenlijke zaken in ons leven kunnen richten of dat we erdoor in een passieve roes terecht komen en juist weinig menselijks (of waardevols) meer overhouden. Uiteindelijk is dit een persoonlijke vraag: hoeveel extra moeite willen we doen, bijvoorbeeld om het beheer van eigen gegevens zelf in de hand te hebben, om op de langere termijn niet op te gaan in een elektronisch symbiotisch panopticum.

Verantwoording en dank

De gedachtengang die in dit boekje uitgewerkt wordt heeft zich de afgelopen jaren gevormd op basis van de literatuur en van discussies met collega's, vrienden en toehoorders (bij voordrachten) en andere geïnteresseerden. Dit boekje is niet zodanig opgezet dat bij iedere gedachte de directe bron vermeld wordt—zo ik die al ken. Maar het moge duidelijk zijn dat ik schatplichtig ben aan velen, die ik bij deze wil danken. Expliciet wil ik echter Marcel Becker, Jaap-Henk Hoepman, Ronald Leenes en Joke Mol noemen voor waardevolle commentaar op een eerdere versie. De verantwoordelijkheid voor deze presentatie, en voor de fouten daarin, ligt natuurlijk geheel bij de auteur.

Tenslotte wil ik nog enige woorden weiden aan het open, gratis karakter van deze publicatie. Aanvankelijk, bij het schrijven van deze tekst, zat ik nog vast aan de traditionele gedachtengang dat een commercieel boekwerkje de beste uitingsvorm zou zijn. Daar is langzaamaan verandering in gekomen, enigszins geholpen door een afwijzing van een uitgever. In het huidige internettijdperk komt *mindshare* voor *marketshare*. De doelgroep wordt het beste bereikt via een (aanvankelijk) gratis product, waarbij even-

tuele inkomsten pas later bij brede verspreiding via additionele diensten verkregen worden. Een goed voorbeeld is internettelefonie via het gratis programma *skype*. Nu heb ik niet de intentie of de illusie dat dit geschrift mijn materiële rijkdom wezenlijk zal vergroten[5]. Het onderwerp leent zich nu eenmaal uitstekend voor moderne, gratis verspreiding via internet, waarbij optimaal gebruik gemaakt wordt van de bestaande individuele autonomie: iedereen is zijn eigen uitgever. Ook heeft de verspreiging in elektronische vorm praktische voordelen: er kan makkelijk in het document gezocht worden (daarom ontbreekt een index) en de erin opgenomen weblinks (URLs) zijn klikbaar. Met deze vrije beschikbaarstelling hoop ik zo veel mogelijk lezers te bereiken en discussie in gang te zetten (en verbeteringen snel te kunnen opnemen). Tegelijkertijd neem ik voor lief dat deze vooralsnog experimentele verspreidingswijze waarschijnlijk enige afbreuk zal doen aan de status van het werk. Het gaat me echter vooral om de inhoud.

Geheel regelloos is deze publicatie echter niet. Gebruiksrechten zijn vastgelegd via de *Creative Commons*[6], waarbij het iedereen vrijstaat dit werk (in z'n geheel) te kopieëren en te verspreiden (of te *hosten*) voor niet-commerciële doeleinden, maar waarbij verandering of bewerking (bijvoorbeeld vertaling) niet is toegestaan. Ook is dit geschrift geregistreerd via een ISBN nummer en gedeponeerd bij de Koninklijke Bibliotheek in Den Haag. Het is dan ook bedoeld als meer dan een spontane blog. Voor eventuele verwijzingen suggereer ik (een variatie op) het formaat:

> B. Jacobs, *De Menselijke Maat in ICT*, versie ??, jaar ??. Beschikbaar via `www.cs.ru.nl/B.Jacobs/MM/`.

waarbij de vraagtekens '??' nader ingevuld moeten worden. Het eerste publieke versienummer is 1.0, van januari 2007. Serieuze reacties zijn welkom op het emailadres `B.Jacobs@cs.ru.nl`.

Nijmegen, Januari 2007

[5] Enige indirecte extra materiële opbrengst is ook hier mogelijk, bijvoorbeeld in de vorm van boekenbonnen, flessen drank of etentjes bij hieruit voortvloeiende lezingen. Algemener zou mijn *marketshare* in het maatschappelijke debat (of in het onderwijs) erdoor toe kunnen nemen, mogelijk meer dan via een beperkte commerciële oplage.

[6] De licentie is *Naamsvermelding-NietCommercieel-GeenAfgeleideWerken*, zie `http://creativecommons.org/licenses/by-nc-nd/2.5/deed.nl`.

Inhoudsopgave

Deel I

Introductie

Hoofdstuk 1

De taal

De wereld is veranderd sinds ‘9/11’, de korte aanduiding voor de aanslagen in Amerika van 11 september 2001. Er is internationaal veel meer aandacht gekomen voor veiligheid en terrorisme. Vanzelfsprekendheden zijn verdwenen en het onderlinge wantrouwen is toegenomen. Nieuwe wetten zijn aangenomen om de opsporingsdiensten meer armslag te geven en om onze westerse maatschappijen beter te beschermen. Daarbij is het kennen en controleren van individuen (met name reizigers) belangrijker geworden, met het gerechtvaardigde doel om mogelijk kwaadwillenden in een vroeg stadium te herkennen, en om uitvoering van hun plannen te verhinderen.

Het politieke taalgebruik (*discours*) is ook veranderd, met fermheid als populaire houding. Hieronder zullen een aantal van de clichés uit dit nieuwe taalgebruik besproken worden. Ze zijn niet allemaal volstrekt nieuw, maar hebben sinds 9/11 wel een nieuwe lading gekregen. Er zullen daarbij een aantal vragen opgeworpen worden die sturend zullen zijn voor de rest van dit boek.

Wie niets te verbergen heeft, heeft ook niets te vrezen

Deze uitspraak is populair in politiekringen. De meest voor de handliggende lezing van de uitspraak is namelijk: wie niets te verbergen heeft *voor de politie*, heeft ook niets te vrezen *van de politie*. Eraan ten grondslag ligt een naïef vertrouwen in de voordelen van transparantie. Wanneer alles over mensen bekend is hoeven ze ook niets te vrezen—van de politie. Ook is hier sprake van groot vertrouwen in deugdelijkheid van beheer, namelijk dat de politie al de beschikbare informatie over individuen ‘streng maar rechtvaardig’ zal behandelen. Bewust lekken, slordigheid, omkoping, misbruik van gegevens of verandering van regime worden buiten beschouwing gelaten.

Gekoppeld aan deze uitspraak komt vaak de claim: “Ik heb niks te verbergen!”. Mijn favoriete reactie daarop is een rechtstreekse vraag: “OK, vertel dan maar eens wanneer je voor het laatst echt te veel gedronken hebt. Of wanneer je voor het laatst gemasturbeerd hebt?” Soms komt er dan een schaamteloos antwoord, maar meestal is de reactie dat het daar niet over gaat. Maar waar gaat het dan wel over? Welke zaken zouden we wel, en welke zouden we niet hoeven te verbergen om niks te vrezen te

hebben? Dit is een fundamentele vraag die nog vaak zal terugkomen. In dit stadium kunnen we opmerken dat de meesten van ons—de volstrekt schaamteloze enkeling daargelaten—terecht zaken voor zichzelf willen houden.

Privacy is de schuilplaats van het kwaad

Deze uitspraak sluit nauw aan bij de vorige. De onderliggende gedachte lijkt ook hier te zijn dat datgene wat—onder het mom van privacy—verborgen gehouden wordt de basis vormt voor allerlei ongewenste activiteiten. Dit is een opmerkelijk negatieve interpretatie van privacy. Men zou misschien wel net zo goed de tegenovergestelde uitspraak kunnen verdedigen: privacy is de bron van al het goede. Waarom hebben we daar geen oog meer voor? Wat is eigenlijk de rol van privacy?

Het minste dat nu gezegd kan worden is dat de negatieve interpretatie botst met de huidige wetgeving, waarbij het belang van privacy niet alleen in de grondwet staat (artikel 10: “Ieder heeft, behoudens bij of krachtens de wet te stellen beperkingen, recht op eerbiediging van zijn persoonlijke levenssfeer”), maar natuurlijk ten grondslag ligt aan de uitgebreide Wet Bescherming Persoonsgegevens (Wbp).

We moeten privacy opofferen voor veiligheid

Ook deze uitspraak past in de bovenstaande lijn: indien privacy afgeschaft wordt kunnen er onder dat mom geen kwaadaardigheden meer stiekem uitgedokterd worden zodat de politie meer informatie bezit en effectiever op kan treden, waardoor de veiligheid toeneemt. Een goede vraag is echter: veiligheid voor wie? Het lijkt te gaan om publieke veiligheid, voor ons allemaal. Je kunt je echter terecht afvragen of individuele veiligheid wel gebaat is bij het opheffen van privacy. Te denken valt aan vrouwen in een blijf-van-mijn-lijf-huis. Hun persoonlijke veiligheid is vaak juist afhankelijk van het verborgen houden van hun precieze verblijfplaats. Het is niet moeilijk meer van zulke voorbeelden te geven waaruit blijkt dat privacy juist essentieel is voor persoonlijke veiligheid. Te denken valt aan politici, die het risico lopen door burgers al te assertief benaderd te worden, bijvoorbeeld met kogelbrieven[1].

Mensen hechten niet (meer) aan privacy

Deze uitspraak lijkt gegrond: de beste manier om aan persoonlijke gegevens (over inkomen, aard van het werk, gezinssamenstelling, bestedingspatronen, voorkeuren etc.) te komen is om een prijsvraag uit te schrijven waarbij deelname vereist dat een lijst persoonlijke vragen beantwoord wordt. Zelfs voor de geringste kans op de onbenulligste prijs zijn veel mensen bereid allerlei intieme details te openbaren. Daarnaast levert

[1] In november 2006 verschenen luchtfoto’s uit *Google Earth* van de huizen van verschillende Nederlandse politici kortstondig op de website `www.casabobo.nl`—die inmiddels een geheel andere rol heeft. Die foto’s zijn echter zeer snel weer weggehaald, ter bescherming van de privacy en/of persoonlijke veiligheid van betrokkenen.

de invoering van privacybeperkende maatregelen in het kader van terrorismebestrijding over het algemeen weinig protest op. Ook zien we een generatie van jongeren die enthousiast persoonlijke profielen op het web publiceert, bijvoorbeeld op vriendensites zoals *hives* of *myspace*. Inmiddels wordt daar niet alleen door de politie dankbaar gebruik van gemaakt bij het opsporingswerk, maar ook door werkgevers bij de selectie van sollicitanten. Stoer doen over het eigen innamevermogen (of andere capaciteiten) kan dan vergaande gevolgen hebben.

Is het inderdaad zo simpel dat men niet meer om privacy geeft? Een feit is dat bewust omgaan met je persoonlijke gegevens en nagaan wat anderen er allemaal mee doen een dagtaak geworden is. Vaak worden details ook niet bekend gemaakt. Wie weet wat Albert Heijn precies doet met de gegevens over het koopgedrag van klanten die via de bonuskaart verzameld worden? En aan wie zulke gegevens beschikbaar gesteld worden?[2] De Wet Bescherming Persoonsgegevens (Wbp) stelt eisen aan de omgang met zulke gegevens, en geeft recht op inzage en correctie. Maar dat recht heeft meer te maken met principes dan met de praktijk.

Bewaking van de eigen privacy is lastig, en wordt ons ook niet makkelijk gemaakt. Wanneer telefoons gewoon twee belknoppen hadden—een voor bellen met privacy en de andere voor bellen zonder privacy—lijkt mij dat de meeste mensen eenvoudigweg voor privacy zouden kiezen[3]. Waarom is onze infrastructuur niet op een zodanige wijze ingericht? Moeten we over die inrichting niet beter nadenken, en de keuzes die nu gemaakt worden niet openlijker bespreken? Deze tekst wil daartoe bijdragen.

Ondanks dat het steeds lastiger wordt om privé gegevens te beheren meen ik dat mensen vanzelfsprekende (en gerechtvaardigde) verwachtingen hebben met betrekking tot privacy—net zoals men er vanuit gaat dat briefverkeer geheim is. Er is nog steeds grote terughoudendheid in het zomaar verstrekken van eigen medische gegevens. En van de gezondheidszorg wordt verwacht dat men zorgvuldig met zulke gegevens omgaat. Ook lijken veel mensen hun financiële gegevens als zeer persoonlijk te beschouwen. En beleving van geloof of sexualiteit behoort voor de meesten van ons tot de intieme persoonlijke levenssfeer waar weinig anderen iets mee te maken hebben.

Naast een zekere slordigheid zien we bij de jongere generatie ook een grotere bewustheid van (elektronische) identiteiten, en een soepelere omgang daarmee. Excessen daargelaten weten de meeste jongeren zeer goed dat enkel een naam geen enkele betekenis heeft op MSN, en dat communicatie met onbekenden risico’s met zich meebrengt (bijvoorbeeld op chantage). Een ander voorbeeld: ik neem mijn mobiele telefoon nog steeds op met de traditionele begroeting “hallo, met Bart Jacobs”. Ik zie jongeren om

[2] Op de website `www.albert.nl` kun je op basis van een bonuskaartnummer de bijbehorende aankopen van de maand daarvoor bekijken. Wanneer je dat van huis uit doet met je eigen bonuskaartnummer schenk je Albert Heijn ook nog je IP-adres—tenminste, wanneer je de herkomst van je webverzoek niet afschermt via een *anonymizer* zoals Tor. Wanneer Albert Heijn dan met je internet provider om de tafel zou gaan zitten kunnen ze gezamelijk een nog uitgebreider profiel van je maken: niet alleen van je eetgedrag maar ook van je surfgedrag.

[3] Het zou ook interessant zijn om te weten hoe vaak mensen op de “privacy” belknop zouden drukken als de kosten zeg een cent per minuut hoger zouden zijn.

mij heen die honderden nummers in hun telefoonlijst hebben en alleen opnemen wanneer de beller op die eigen lijst voorkomt, en dan met een moderne begroeting als “hoi Sophie, hoe is het?”. Dit geeft een zorgvuldige afscherming en effectieve bescherming tegen ‘spamtelefoontjes’ of andere vormen van last. De aanstormende generatie is gewend zichzelf centraal te plaatsen en verwacht dat ICT hen daarbij ondersteunt. Daarbij gaan ze soepel en ongrijpbaar om met identiteiten: “hier heb je een SIM met nog 20 Euro beltegoed; dan staan we kiet!”.

Iedereen moet in de centrale databank

Om mensen beter in de gaten te kunnen houden moet je in staat zijn ze te herkennen, bijvoorbeeld op een filmpje van een surveillancecamera, in een afgeluisterd telefoongesprek, of aan de hand van nagelaten sporen. Terroristen zijn enge onbekenden. Het klinkt dan aantrekkelijk om een grote databank op te zetten waar iedereen in zit—inclusief de terroristen. Vervolgens lijkt het probleem een stuk makkelijker, omdat we de terroristen alleen nog maar hoeven te herkennen in die databank. Daarvoor moet dan zogenaamde slimme software zorgen.

Helaas werkt het niet zo. Terroristen doen juist hun best om niet herkenbaar te zijn en niet op te vallen. Groots opgezette miljardenverslindende projecten zoals het Amerikaanse *US Visit* programma, waarbij van alle buitenlanders die de VS binnenkomen een foto en vingerafdrukken worden afgenomen, hebben (zover publiekelijk bekend) er slechts toe geleid dat enkele domme criminelen als kleine visjes gevangen werden. Het zou wellicht effectiever zijn om al dat geld in traditionele misdaadbestrijding te investeren.

Niemand heeft iets te vrezen van correcte identificatie

Ten grondslag aan de roep om centrale databanken ligt een gevoel dat burgers onvoldoende bekend zijn bij de overheid, en in het bijzonder bij de instanties die zich met opsporing en verstoring bezig houden. Dit gevoel krijgt soms de meer radicale uiting in de roep om iedereen een chip in de nek te schieten. Daarbij wordt waarschijnlijk gedacht aan een zogenaamde RFID-chip die op afstand uitleesbaar is en bij ieder individu een uniek nummer weergeeft, zoals bijvoorbeeld het Burger Service Nummer (BSN). Dat kan nog handig zijn ook: als je bij een loket komt zien ze meteen wie je bent, en verschijnt je dossier op het scherm. In iets gematigder vorm zijn er vergelijkbare plannen om allerlei objecten van RFID-chips te voorzien, van kleding en pakjes scheermesje in de winkel tot fietsen en nummerplaten van auto’s.

Zelden wordt er daarbij stilgestaan bij de risico’s die zo’n eenvoudige identificeerbaarheid voor individuen met zich meebrengt. Een heethoofd die het op een locale wethouder, een kamerlid, een ondernemer, of een minister gemunt heeft kan eerst een keer onopvallend langs deze persoon lopen om zijn of haar unieke nummer te scannen. Vervolgens kunnen een aantal automatische bommen geplaatst worden op locaties waar het beoogde slachtoffer wel eens voorbij komt. Die bommen zijn zodanig selectief afgesteld dat ze alleen exploderen wanneer ze het nummer van de gescande chip voorbij zien komen. Er is achteraf geen spoor van de dader. We kunnen er gerust van uitgaan dat afrekeningen in het criminele circuit (of daarbuiten) een groter high-tech gehalte krijgen en dat ook kwaadwillenden dankbaar gebruik zullen maken van deze identificatiemogelijkheden: de RFID-chip in een nummerplaat van de auto van het slachtoffer activeert de bom. Mogelijk pas wanneer dat soort aanslagen echt plaatsvinden zien we de risico’s van de ondoordachte roep om universele herkenbaarheid. Misschien moeten we nu alvast wat beter nadenken. Het bureaucratische ideaal van volledige controle bedoeld om risico’s uit te bannen draagt eigen risico’s in zich. Een zekere mate van ongrijpbaarheid is niet alleen wenselijk maar ook nodig.

Beter tien mensen onschuldig in de cel, dan één terrorist die vrij rondloopt

De achterliggende idee bij deze uitspraak lijkt te zijn dat men het bij terrorismebestrijding niet zo nauw moet nemen. Men moet breed inzetten, niet al te zorgvuldig zijn, en *collateral damage* als noodzakelijk accepteren. De focus enkel op de bad guys lukt niet, waar de good guys maar onder moeten lijden. Dit wordt gepresenteerd als een prijs die maar geaccepteerd moet worden. Als jij toevallig één van die onschuldigen in de cel bent heb je vette pech.

Deze uitspraak appelleert op een gevaarlijke manier aan onderbuikgevoelens en gaat juist tegen onze rechtstaat in die op het omgekeerde idee van *beyond reasonable doubt* gebaseerd is: niemand is schuldig tenzij expliciet bewezen voor een rechter, waarbij men vrijuit gaat in geval van twijfel. De uitspraak suggereert dat we de normen voor bewijsvoering moeten aanpassen, en bij terrorismebestrijding ook tot opsluiting moeten overgaan bij twijfelachtig bewijs.

Op de achtergrond speelt een geleidelijke maar fundamentele verschuiving. Traditioneel is het zo dat je eerst als verdachte aangemerkt dient te worden (op basis van een redelijk vermoeden) voordat jouw fundamentele rechten geschonden mogen worden in een opsporingsonderzoek, bijvoorbeeld via huiszoeking of tappen van telefoongesprekken. Hierbij gaat het dus om eerst selecteren (van de verdachte) en dan pas verzamelen. Met moderne technieken wordt het steeds eenvoudiger—en gewoner—om deze volgorde om te draaien: eerst over iedereen met een sleepnet informatie verzamelen, en vervolgens pas selecteren van wie de informatie gebruikt wordt. Dit ziet men duidelijk bij het Europese voornemen tot opslag verkeersgegevens, waarbij het internetgebruik en belgedrag van alle 500 miljoen Europeanen voor langere tijd opgeslagen dient te worden. We zijn allemaal bad guys geworden.

Wil jij dan verantwoordelijk zijn voor de volgende terroristische aanslag?

Deze uitspraak is natuurlijk de meest effectieve manier om iedere rationele discussie om zeep te helpen. Dit boek beoogt echter om zo’n teloorgang nog even uit te stellen. Het wil de (vooral) technische mogelijkheden verkennen om de fundamenten van onze rechtstaat te verdedigen en mogelijk zelfs te versterken, waarbij zorgvuldigheid

en aandacht voor individuen centraal staan. De achterliggende gedachte is dat de uitdaging van terroristen om onze eigen op individuele autonomie gerichte normen en waarden te ondermijnen beter bestreden kan worden via verdediging en versterking dan via afbraak van de rechtstaat. We laten ons toch niet door terroristen voor hun karretje spannen, zodat ze kunnen zeggen: zie je wel hoe verdorven westerse maatschappijen met hun eigen burgers omgaan? Terroristen dagen ons immers uit juist die waarden te ondermijnen waarvan we het hardst roepen dat we ze verdedigen. Laten we ze dan ook verdedigen!

Hoofdstuk 2

De verandering

Mijn studietijd viel in het begin van de jaren tachtig. De sfeer was grauw en grimmig. Lubbers was begonnen aan zijn zakelijke saneringsbeleid en kernwapens en kruisraketten domineerden de nationale en internationale politiek. Ik had het idee in een lege periode te leven: de roerige jaren zestig waren echt voorbij, de generatiekloof was niet diep meer, en schokkende of inspirerende technologische ontwikkelingen waren er ook niet.

De studiedruk was in die periode niet zo hoog, en ook de studiefinanciering was relatief comfortabel. Ik heb in die periode braaf gestudeerd (wiskunde en filosofie), maar ook gereisd: goedkoop, vaak liftend, onbevangen en open voor nieuwe indrukken en perspectieven. Hieronder volgen twee korte verslagen van zulke reizen, bedoeld als illustratie van wat voor mij wezenlijke indrukken zijn geweest, en tegelijkertijd als achtergrond om aan te geven wat er gaandeweg veranderd is.

Mijn vader kwam uit een goed katholiek gezin, vanwaaruit één van de zoons het klooster inging. Deze heeroom is in de missie terechtgekomen, en wel in Pakistan. Toen ik hem in Nederland een keer ontmoette nodigde hij me uit voor een bezoek. Ik heb hem inderdaad bezocht, samen met een goede studievriend. We zijn drie maanden weg geweest, waarvan uiteindelijk slechts drie weken in Pakistan, en de rest van de tijd in India. We kwamen er snel achter dat in Pakistan zo'n beetje al het leuke en aangename verboden was. Ik herinner me dat er in die tijd ophef in de Pakistaanse pers was omdat een of andere Engelse cricketer over het land had gezegd: *you wouldn't send your mother in law there*. India was aangenamer en letterlijk veel kleurrijker. Het land was nog economisch gesloten, en vol met ambassadors en riksja's. We hebben een klassieke tour afgelegd langs Bombay, Goa, Mangalore, Varanasi, Agra, Delhi en Jaipur. We reisden met rugzak, in rammelende bussen (bij drukte door het raam naar binnen) en vooral veel treinen (derde klas, eindeloos traag, maar steeds vol verrassingen).

We waren in die tijd echt weg: onbereikbaar en ontraceerbaar. We hebben niet gebeld met familie of vrienden, maar stuurden wel een paar kaarten en brieven. Verzendtijd (of aankomst überhaupt) was onvoorspelbaar. Andersom hebben we een aan-

tal brieven gekregen via *poste restante*. Het is nu bijna niet meer uit te leggen wat dat inhield: in Nederland werd de brief verzonden met als bestemming bijvoorbeeld: “Bart Jacobs, Central Post Office, New Delhi, Poste Restante”. De brief werd dan bij aankomst een tijdje bewaard op het postkantoor in Delhi totdat ik hem op kwam halen. We hebben op zo’n manier inderdaad een aantal keer post gehad, maar naar later bleek, ook enkele brieven gemist. Misschien liggen ze nog ergens te wachten.

De NRC-columnist Frits Abrahams beschreef in november 2003 dat zijn dochter na haar eindexamen een grote reis door Zuid-Oost Azië maakte. Ongeveer iedere dag schreef ze een email vanuit een internetcafé over haar ervaringen. Abrahams vergeleek dit regelmatige contact met de onbereikbaarheid van vroegere reizen. Hij beschreef de huidige situatie als een gemengd genoegen, omdat de achterblijvende ouders machteloos meekeken bij alles wat niet goed ging of niet goed dreigde te gaan.

Het is me er niet om te doen om het één of het ander beter of slechter te noemen. Maar wel om het benoemen van de ervaring van volledig los zijn van bestaande verbanden, en de daarbij horende vormen van controle, monitoring, steun en raad. Het is zo volledig anders dan de huidige situatie waarin de meesten van ons altijd bereikbaar willen of moeten zijn, en waarin bijna al onze handelingen elektronisch traceerbaar zijn—betalingen, telefoontjes, email, websurfing, (digitaal) TV-kijken, reizen (via OV-chip of surveillance camera’s)—en waarin we uit veiligheidsoverwegingen ook steeds nadrukkelijker in de gaten gehouden worden. De privacy en anonimiteit die hoorde bij de toenmalige reis naar het subcontinent is eigenlijk niet meer realiseerbaar. Destijds was ik me er absoluut niet van bewust dat die ervaring van vrijheid en ongebondenheid zo bijzonder zou blijken te zijn.

Verbondenheid met eigen cultuur en met naasten is belangrijk. Daarbij is het meen ik ook waardevol om af en toe ‘los’ te kunnen zijn. Nu en in de toekomst betekent dat om af en toe alle sensors los te kunnen trekken, om even rustig na te kunnen denken, net teveel te drinken, te masturberen, of gewoon een potje te kunnen janken. Maar, zeggen de wantrouwende hardliners dan, hoe weten we als de sensors los zijn of u wel echt een potje zit te janken en niet stiekem een terroristische aanslag aan het voorbereiden bent. Misschien moeten we uw activiteiten toch maar blijven registreren! Hoe ver willen we het hierin laten komen?

Andere reizen, maar met dezelfde studievriend, leidden naar West en Oost Berlijn. Dat was ruim voor 1989 en de *antifaschistischer Schutzwall* stond nog stevig overeind. We hebben steeds gelift, waarbij vooral het laatste stuk van de reis avontuurlijk was: de ongeveer 200 kilometer over de *Transitstraße* door het communistische Oost-Duitsland van nabij Hannover naar West-Berlijn. Je moest dan één lift zien te krijgen, want onderweg uitstappen was verboden. Je moest die afstand sowieso in een paar uur afleggen, want anders kwam je in de problemen. Dat werd allemaal bijgehouden. In feite was het nooit moeilijk om op die snelweg een lift te krijgen want mensen reisden daar niet graag alleen—vooral vrouwen niet. De doorgangen door de muur (bij Helmstedt-Marienborn en bij Dreilinden) waren indrukwekkend. De sfeer was militairistisch en dreigend, en de controles waren aggressief en intimiderend.

Eenmaal in West Berlijn was het leven weer herkenbaar, ook al was de beklemmende sfeer van de muur nooit ver weg. Mijn reisgenoot, hongerig na een avondje stappen, heeft Berlijnse vrienden ooit versteld doen staan met de onvergetelijke vraag *ob mann hier auch irgendwo aus der Mauer essen kann*.

Van één van die reizen herinner ik me een dagbezoek vanuit West Berlijn aan Oost Berlijn nog zeer goed. We hadden ons onderdak in West Berlijn niet goed geregeld, en sliepen in een rommelig en chaotisch kraakpand in de wijk Kreuzberg. We lieten daar overdag onze spullen liever niet achter. In al onze naïviteit verschenen we dus met volle bepakking aan de Oost-Duitse grens. Daar vielen we direct op als verdacht. We zijn uitgebreid ondervraagd over waarom we toch een rugzak met slaapzak nodig hadden voor een bezoek van enkel een dag. Op een of andere manier hebben we ons daar toen uitgekletst—oprechte naïviteit geeft een zekere onkwetsbaarheid—en na verplichte omwisseling van 25 West-Marken tegen 25 Ost-Marken (ten bate van de oosterse deviezenvoorraad) mochten we doorlopen. Het zat me echter toch niet lekker, en ik heb bij de grensovergang goed rondgekeken. Al snel bleek dat we gevolgd werden. Na een paar honderd meter werden we aangesproken met de vraag of we wilden wisselen, tegen een gunstiger koers. We wisten dat dat illegaal was, maar hadden het ooit wel eerder gedaan. Ik voelde nu echter nattigheid, vermoedde uitlokking, en heb in mijn beste Duits aangeven dat we zoiets *grundsätzlich* niet deden. De ‘wisselaar’ droop af, maar het schaduwen ging door, de hele dag lang. Het was iets dat we nog nooit meegemaakt hadden, en ook in de verste verten niet kenden uit een Nederlandse context: een staat die individuen zo nadrukkelijk en intimiderend in de gaten hield. Het was verontrustend en beklemmend. Maar we waren studenten, en in een balorige bui zwaaiden we een paar keer naar onze achtervolger. Daarna leek iemand anders het over te nemen. We hebben echter verder niks bijzonders gedaan—*Das Kapital* spotgoedkoop gekocht, maar nooit gelezen—en zijn ’s avonds zonder problemen teruggekeerd in West Berlijn.

Op zich ging het hier natuurlijk om een onbenullig voorval, maar de ervaring was er, en het gevoel van beklemming en onvrijheid had postgevat. Het gaf me een beter oog voor de betekenis van individuele vrijheid, niet alleen om te doen en laten wat je wil, maar ook om je niet gecontroleerd en geïntimideerd te voelen. Ik realiseerde me dat het geen vanzelfsprekende luxe is om je niet bij al je gedragingen te hoeven afvragen of dit mogelijk afwijkend is en additionele (staats)controle over je afroept—met alle mogelijke negatieve consequenties vandien. Het werd me nadrukkelijk duidelijk dat de Nederlandse samenleving (natuurlijk niet als enige) gebaseerd is op een zekere mate van wederzijds vertrouwen: burgers weten waar ze aan toe zijn met de overheid, en de overheid vertrouwt de burgers binnen redelijke grenzen en laat ze daarin vrij.

Inmiddels ben ik in mijn leven het gevoel kwijt geraakt in een saaie tijd te leven zonder grote historische gebeurtenissen. Ik denk aan 11/9 en 9/11 (val van de Muur op 9 november 1989 en de aanslagen in New York en Washington op 11 september 2001), maar ook aan de opkomst van internet en mobiele telefonie, en het algehele ‘plat’ worden van de wereld. Wat ik trouwens als een zeer opwindende historische

gebeurtenis beschouw—en graag mee zou maken—is contact met ander, buitenaards leven. Maar dat terzijde.

Het beklemmende gevoel veroorzaakt door de Berlijnse ervaring is jarenlang ver weg geweest. Maar de laatste paar jaren komt het soms ineens weer terug, in mijn eigen omgeving. De sensors worden steeds dichter op de huid geplaatst. Soms spreek ik mensen over de telefoon—een onderzoeksjournalist, advocaat, activist, of iemand uit de beveiligingswereld—waarbij ik bijna zeker weet dat het gesprek afgeluisterd wordt. Ik spreek daarom ook af en toe bewust persoonlijk met mensen af, om open communicatie via telefoon, email of chat te vermijden. Ik ben me ervan bewust wanneer mijn mobiele telefoon aanstaat, en wanneer mijn locatie dus bepaald kan worden. Soms zet ik het mobieltje met opzet uit, niet alleen omdat ik niet gebeld wil worden, maar ook omdat ik niet wil dat er in grote databanken opgeslagen wordt waar ik me op dat moment bevind. Ik ben me nadrukkelijk bewust van de zoektermen die ik bijvoorbeeld bij Google intyp—alles wordt opgeslagen, met mij geassocieerd en komt mogelijk ooit weer boven water—en van de websites die ik bezoek, met al hun invulformulieren. Ik gebruik met enige regelmaat beschermende programma's (zoals een zogenaamde *anonymizer* als Tor) waardoor de herkomst van mijn webverzoeken gemaskeerd wordt. Voor een deel komt deze beklemming (of paranoia, zo u wil) door het soort werk dat ik doe op het gebied van computerbeveiliging, maar voor een niet onaanzienlijk deel is er ook echt iets wezenlijks veranderd in onze eigen samenleving. Dat komt niet alleen door 9/11, maar ook door het voortgaande gebruik van ICT en door de manier waarop we deze ICT-infrastructuur zelf inrichten.

Hoofdstuk 3

De keuzes

Nederland ligt regelmatig lam door de files op de snelwegen. Er wordt al jaren gepraat over rekeningrijden als oplossing: vervang de huidige *flat rate* wegenbelasting door een flexibeler stelsel waarin de automobilist betaalt naar gebruik. Dit klinkt rechtvaardig en geeft een financiële stimulans om minder te rijden. Deze stimulans kan heel gericht ingezet worden om typische filetrajecten of drukke dagdelen extra duur te maken en zo de verkeersstromen beter te kunnen verdelen.

Begin 2001 heeft de toenmalige minister van verkeer Netelenbos de nationale ICT-goeroe van destijds, Roel Pieper, gevraagd dit idee nader uit te werken. Hij kwam toen, met hulp van anderen, met zijn *MobiMiles* plan dat als volgt in elkaar stak. Monteer in iedere auto een speciaal kastje met daarin een GPS ontvanger (voor locatiebepaling) en een GSM voor communicatie. De auto 'weet' dan zelf waar hij is, en kan die informatie doorgeven aan de betreffende overheidsdienst om een passende heffing te berekenen. Dit is een eerste, naïeve aanpak, die overigens niet in deze vorm bij *MobiMiles* voorkomt.

Men realiseerde zich namelijk direct dat hierbij fundamentele aspecten van privacy in het geding zijn: moet de overheid wel weten waar welke auto zich op welk moment bevindt? Dit klinkt wel erg sterk als Big Brother. Afgezien van deze terechte zorg was men zich er ook van bewust dat privacy argumenten als bezwaar aangegrepen zouden kunnen worden door allerlei groepen in de samenleving die zich normaal helemaal niet zo druk maken om privacy maar die het hele plan van rekening rijden absoluut niet zien zitten.

In zulk soort situaties dient men zich de fundamentele vraag te stellen: wat is eigenlijk het doel, en wat is daarvoor de minimaal noodzakelijke hoeveelheid informatie? Het doel is in dit geval om het gebruik van de snelwegen op een of andere manier te kwantificeren, aan de hand van (mogelijk flexibele) tarieftabellen. Daarvoor heb je niet nodig waar de auto zich bevindt, maar enkel hoeveel hij in welke tariefklasse heeft gereden. De oplossing is om de hele zaak te *decentraliseren*: zet die tabellen in de kastjes (in de auto's), en maak het desgewenst mogelijk om die tabellen via GSM (beveiligd) te verversen. Waar dit op neerkomt is dat Nederland verdeeld wordt in, zeg, rode, groene, gele en blauwe wegen (ieder met een eigen tarief), en dat de kastjes

iedere maand doorgeven hoeveel kilometer op welke kleur gereden is. Dat geeft precies voldoende informatie om de heffing te berekenen. Een heldere, begrijpelijke en privacy-vriendelijke oplossing, waarbij mensen niet onnodig getraceerd worden.

Voor de volledigheid moet ik zeggen dat er nog een ander aspect aan dit *MobiMiles* plan zit dat ik hier echter minder benadruk, namelijk de controle op de naleving. Mensen zouden hun kastjes mogelijk uit kunnen zetten, bijvoorbeeld door de stroomvoorziening te onderbreken. Die controle was door Pieper steekproefsgewijs voorzien, via verplaatsbare poortjes langs de snelwegen waarbij aan de kastjes in voorbijkomende auto's draadloos bepaalde kritische vragen gesteld konden worden. Bij een onjuiste reactie kon de auto dan verderop aangehouden worden.

Dit oorspronkelijke plan voor rekeningrijden sneuvelde al in 2002 bij de formatie van het eerste kabinet Balkenende. De zaak heeft een tijd stil gelegen, maar recentelijk is het thema weer op de politieke agenda gekomen. De komende jaren zal een nieuw systeem uitgedacht en ingevoerd worden. Hoe dat er precies uit gaat zien is vooralsnog niet duidelijk. Ik houd mijn hart vast dat dit alsnog een *centralistisch* systeem wordt, waarbij de locatie van iedere auto in een centrale databank permanent wordt bijgehouden en de basis vormt voor de heffingen. Ik durf te voorspellen dat de noodzaak van een centrale databank beargumenteerd zal worden vanuit bestrijding van terrorisme en zware criminaliteit.

Wanneer zulke zware argumenten op tafel komen worden een redelijke discussie en afweging moeizaam. Om te beginnen is de centrale databank niet nodig voor het heffen van de belasting, zie het oorspronkelijke plan van Pieper. Verder zullen terroristen en zware criminelen er heus wel op letten dat ze op zo'n manier niet getraceerd worden, bijvoorbeeld door regelmatig van auto te wisselen en bij een delict een gestolen auto te gebruiken (zoals nu ook al vaak voorkomt). Er zullen hooguit een aantal domme criminelen mee tegen de lamp lopen. Maar de gewone goedwillende burgers worden zo weer met een nieuw systeem—naast bijvoorbeeld de OV-chipkaart—opgescheept waarmee hun gedrag nauwlettend gevolgd kan worden. Nog meer sensoren op je lijf! Daarbij komen nog de risico's van centrale opslag. Stel de databank wordt gehackt, en er blijkt dat bepaalde politici vaak in hoerenbuurten komen. Dan is het land te klein. Ongetwijfeld zullen er ook fouten in het systeem sluipen. Wat moet je als je op basis van (mogelijk vervalste) gegevens in zo'n databank onterecht beschuldigd wordt? Kafka-achtig!

Het is me hier niet zozeer te doen om rekeningrijden, maar om de achterliggende informatiearchitectuur. Zonder al te veel moeite zijn er tientallen situaties te vinden waar sprake is van vergelijkbare issues rond (de)centralisatie, identificatie en regulering van toegang. Het is van belang dat we ons bewust zijn van deze issues en van de consequenties van deze of gene architectuur, zodat we niet direct de meest voor de handliggende inrichting kiezen maar tot een weldoordachte afweging kunnen komen. We zouden kunnen proberen iets creatiever met de technologie om te gaan en de controle die ermee mogelijk is alleen gericht en selectief in te zetten. Uitgangspunt bij rekeningrijden zou kunnen zijn: decentrale opslag in de kastjes in de auto voor de good guys, en tijdelijke centrale opslag voor de bad guys als gevolg van een gerechtelijk vonnis of een onderbouwde verdenking. Mensen die zich misdragen hebben weten dan dat ze gedurende enige tijd (of misschien wel voor altijd) beter in de gaten gehouden zullen worden. Daar kan een preventieve werking van uit gaan. De gewone burger kan zich blijven koesteren in het vertrouwen dat de overheid hem of haar als onschuldig blijft behandelen totdat het tegendeel bewezen is.

Natuurlijk blijft er het argument dat er met een centrale databank meer te reconstrueren is, met name van een *good guy* die plotseling *bad* geworden is. Maar misschien is dat een redelijke prijs om te betalen als het alternatief is om iedereen als *bad guy* te behandelen en zo een volgend element van vertrouwen uit onze samenleving te slopen. Deze discussie komt terug in Hoofdstuk 15.

We bevinden ons nu in een fase waarin grote ICT-infrastructuren worden uitgedacht en uitgerold die vergaande consequenties hebben voor onze ervaring van autonomie, vrijheid, privacy en controle. We hebben het over paspoorten met chips, rekening rijden, OV-chipkaarten, RFIDs, grootschalig gebruik van biometrie, etcetera. Bij de besluitvorming over zulke projecten spelen veiligheidsargumenten (terecht) een grote rol. Maar er lijkt weinig visie te zijn op waar we op de langere termijn mee bezig zijn, en welke waarden we als essentieel overeind willen houden. Techniek is duidelijk niet waardenvrij. We maken nu essentiële keuzes—bijvoorbeeld over al of niet centraliseren—met vaak eenzijdige argumenten. Over zeg 10 of 20 jaar kijken we terug en vragen we ons af: hoe heeft het zover kunnen komen? *Where did we go wrong?*

Nederland heeft de kennis en technologie in huis om kernwapens te produceren. Er is echter consensus dat we dat maar beter niet kunnen doen. Klonen van mensen is ook zo'n onderwerp waarbij we uiterst terughoudend zijn. Ook op ICT-gebied zien we tekenen van beperking van inzet van technologie, bijvoorbeeld bij stemmachines[1]. Misschien zouden we ons in de inzet van ICT met betrekking tot personen en persoonsgegevens ook iets minder moeten laten leiden door wat technisch mogelijk is, en wat meer door een gedeelde visie op hoe we met elkaar om willen gaan, die past bij onze cultuur. Dit boek wil bijdragen aan zo'n visie, met daarbij nadrukkelijk oog voor de menselijke maat, differentiatie en kleinschaligheid in ICT. In de woorden van Richard Thieme[2]:

> The battle for freedom is not being fought in wars far from home but in the policies en decisions we make personally and professionally about how we will live in a wired world. If those decisions are conscious, deliberate, and grounded in our real values and commitments, we will build communities on-line and off that are open, evolving, and free. If we are manipulated into fearing fear more than the loss of our own power and possibilities, then our communities will be constricted, rigidly controlled, over-determined.

[1] Zie de opgelaaide discussie in de tweede helft van 2006, resulterend in de gedeeltelijke herintroductie van potlood en papier.

[2] Uit zijn column *Computers, Freedom, and Privacy* van 21/2/1998, zie bijv. de verzamelbundel *Islands in the Clickstream: Reflections on Life in a Virtual World* (Syngress Publishing, 2004).

Deel II

Identiteit

Hoofdstuk 4

Identificatie en authenticatie

Traditioneel woonden mensen in kleine gemeenschappen waarin iedereen elkaar persoonlijk kende, het bestuur beperkt en sterk locaal georganiseerd was, en men weinig reisde. Gaandeweg is dat gaan veranderen. Moderne samenlevingen hebben veel verschillende deelnemers, die bovendien zeer mobiel zijn, en hebben complexe vormen van bestuur. Identificatie van individuen is daarbij tegelijkertijd belangrijker en ook moeilijker geworden. Er kan sprake zijn van transacties tussen mensen onderling, tussen burgers en overheden, of tussen klanten en bedrijven die producten of diensten bieden. Vaak vinden zulke transactie plaats zonder direct contact (niet meer *f2f* of *face-to-face*), maar via telefoon, email, of een webformulier. Hoe weet je dan nog wie je aan de andere kant hebt? En hoe zeker moet je dat eigenlijk weten, in een bepaalde situatie? Welke garanties zijn nodig voor het geval dat de transactie niet loopt zoals (door één van de partijen) bedoeld?

Dit hoofdstuk beoogt in vogelvlucht een overzicht te geven van een aantal basisbegrippen en ontwikkelingen op het gebied van identificatie en authenticatie van personen. Het is daarbij niet de bedoeling om in te gaan op de technische details. Wel is een zeker kader noodzakelijk voor de latere beschouwingen. Veel ontwikkelingen hebben te maken met het toenemend gebruik van computers in ons dagelijkse leven. Computers begrijpen alleen heldere instructies: in die situatie, doe dat; zolang zus, doe zo. Deze instructies worden vervat in programmatuur (of software) die door computers uitgevoerd wordt. Wanneer taken dus door computers overgenomen dienen te worden (ofwel, geautomatiseerd worden) is allereerst een heldere beschrijving of formalisatie van de betreffende taak nodig. Dit dwingt ons ertoe om impliciete gebruiken, begrippen en regels expliciet te maken. Vaak komen daarbij onduidelijkheden en ambiguïteiten aan het licht, die vragen om een expliciete keuze of interpretatie. Begripsverheldering is daarom belangrijk in discussies over de inrichting van onze ICT-infrastructuur. Het is een grote uitdaging om op een zodanige manier tot formalisatie te komen dat informele gebruiken en gewoontes er direct in herkend worden. Pas dan kunnen gebruikers goed omgaan met de technologie, is de acceptatie groter en de vervreemding kleiner.

De nadruk in dit boek ligt op de omgang met identiteiten. Primair gaat het daarbij

om identiteiten van mensen. Maar wat algemener kan het ook gaan om identiteiten van apparaten, bijvoorbeeld wanneer twee computers met elkaar communiceren. Meestal kunnen in dat geval menselijke metaforen gebruikt worden.

Identificatie en authenticatie

De begrippen identificatie en authenticatie worden niet altijd helder onderscheiden. Hier zullen we ze als volgt gebruiken: identificatie is *zeggen* wie je bent, en authenticatie is *bewijzen* wie je bent. Een agent die wil weten wie je bent kan je eerst vragen om je te identificeren (je zegt je naam), en vervolgens vragen om je te authenticeren (je toont je paspoort). Bij het inloggen op een computer dient je loginnaam als identificatie, en je wachtwoord als authenticatie. Op eenzelfde manier dient je bankrekeningnummer ter identificatie, en je PIN ter authenticatie. Dat deze begrippen niet altijd helder gescheiden worden blijkt bijvoorbeeld uit de afkorting PIN voor *Personal Identification Number*. PAN zou beter zijn.

Binnen deze begripsopvatting stelt identificatie niet zo veel voor. Iedereen kan zichzelf immers zo noemen als hij of zij wil. Inderdaad, een naam op MSN heeft geen enkele betekenis of bewijskracht. Authenticatie daarentegen heeft veel meer gewicht. Een fundamentele vraag bij iedere transactie is altijd: wie authenticeert zich eerst? Diegene die dat doet geeft immers informatie over zichzelf weg, en maakt zich daarmee mogelijk kwetsbaar. Een risico is bijvoorbeeld diefstal van identiteit, wanneer iemand anders zich als jou voordoet, en op jouw rekening mogelijk allerlei bestellingen doet. In het algemeen is wederzijdse authenticatie als een soort onderhandelingsproces, waarbij de twee partijen stukje bij beetje iets van zichzelf bloot geven. Een gouden regel is dat de sterkere partij het eerste stapje moet doen omdat die partij het minste te verliezen heeft. Natuurlijk kan het een punt van discussie wie de sterkere partij is, maar een redelijk criterium is dat het degene is die het minste risico loopt bij een afgebroken authenticatieproces. In een interactie tussen een individu en de “omgeving” vormt de omgeving meestal die sterkere partij. Indien er geen duidelijk sterkste partij is maakt het niet zoveel uit wie er begint.

Stel een agent op straat ziet reden om uw identiteit te controleren. Die agent is de sterkere partij. U kunt dan ook eerst de agent vragen zich te authenticeren. Dit is volkomen redelijk. Het kan net carnaval geweest zijn, waardoor er veel nepagenten rondlopen. U wil natuurlijk wel zeker weten met een echte agent van doen te hebben voordat u details over uzelf blootgeeft. Sterker nog, volgens geldende regels is de agent verplicht om zich eerst te authenticeren indien u dat wenst. Na succesvolle authenticatie van de agent bent u vervolgens wel verplicht u ook te authenticeren. Daarbij dient de agent trouwens wel een goede reden te hebben om uw identiteit te controleren. Volgens de omschrijving in de wet op de identificatieplicht mag de controle niet willekeurig zijn, maar moet die noodzakelijk zijn voor de uitoefening van de taken van de agent.

Vaak vindt authenticatie impliciet plaats. Veel mensen zullen aannemen dat iemand die een politie-uniform draagt—en zich passend gedraagt—een agent is. Een

dokter hoeft zich zelden te authenticeren: de omgeving en de witte jas zijn meestal voldoende overtuigend. Echter wanneer u met een medische klacht bij een onbekende arts komt kan authenticatie als een onderhandelingsproces plaatsvinden. De arts kan u vragen u eerst te authenticeren, als individu die voldoende verzekerd is: uw naam plus verzekeringsnummer vormt de identificatie, en uw paspoort plus verzekeringskaartje de authenticatie. Vervolgens is het redelijk wanneer u de arts vraagt zich te authenticeren, in ieder geval om uzelf ervan te overtuigen dat u te maken heeft met iemand die medisch onderlegd en bevoegd is. Het zou echter ook andersom kunnen, omdat er hier geen duidelijk sterkste partij is.

Authenticatie hoeft niet noodzakelijk alleen tussen mensen onderling plaats te vinden, maar kan ook tussen mens en machine, of tussen machines onderling. Te denken valt bijvoorbeeld aan het ‘contact’ tussen mij en een geldautomaat. Ik moet mij authenticeren met mijn bankpas en PIN. Wat echter zeer vreemd is dat er geen eerdere expliciete authenticatie van de automaat (als omgeving) plaatsvindt: ik moet er op een of andere manier maar op vertrouwen dat de automaat echt is, terwijl ik er toch voor mij cruciale informatie aan toevertrouw (mijn pas en PIN, en daarmee toegang tot mijn bankrekening). Dit is geen puur theoretisch probleem: meermaals zijn er nepautomaten opgedoken waar mensen in goed vertrouwen hun kaart en PIN aan toevertrouwd hebben, met alle negatieve gevolgen vandien voor hun banksaldo. Banken nemen dit probleem in ieder geval naar buiten toe niet heel serieus. Ze zeggen slechts: u moet goed kijken. Maar waarnaar? Voor betalingen online is zo’n houding zeker inadekwaat. Aan het eind, in Hoofdstuk 21, zal hier nader op ingegaan worden.

Onlangs was ik betrokken bij een transactie via een notaris. Ik moest mij daar authenticeren met mijn paspoort. Daarop vroeg ik de notaris of hij kon laten zien dat hij wel echt de notaris was die hij beweerde te zijn. Hij kon dat niet. Hij wilde wel zijn paspoort laten zien, en vertelde dat hij zijn benoemingsbesluit tot notaris ergens thuis had liggen. Hij was zo professioneel mijn vraag volstrekt legitiem te vinden. Hij sprak zelfs van een omissie in de regelgeving dat hij zich niet hoefde te authenticeren.

Uiteindelijk heb ik de transactie wel ondertekend. Ik vertrouwde op de omgeving (het notariskantoor), zijn naam op het bordje op de deur, en de aanwezigheid van een mij bekende collega van de notaris. Wanneer zulke transacties online gaan plaatsvinden is het echter belangrijk ook in voldoende mate zeker te zijn van de identiteit en/of kwalificaties van de betrokken partijen. De gebruikelijke mechanismen waarin uiterlijk, onmiddelijke nabijheid en gedrag zo’n belangrijke rol spelen zijn dan niet meer toereikend. Ook de integriteit van de authenticatiemiddelen en kwalificaties (zoals benoemingsbesluiten of artsdiploma’s) dient elektronisch geverifieerd te kunnen worden.

Veel van ons handelen blijkt gebaseerd te zijn op vertrouwen. We vertrouwen niet alleen veel verschillende personen, maar ook de kwalificaties die aan die personen toegekend worden (attributen). Waarop is zulk vertrouwen eigenlijk gebaseerd, en hoe zou vertrouwensopbouw in een online wereld plaats kunnen vinden? Dit zijn moeilijke maar uitdagende vragen die het hart van onze (toekomstige) maatschappelijke organisatie raken.

Vormen van authenticatie

Een fundamentele vraag is hoe je authenticeert. Dat wil zeggen, hoe bewijs je dat een bepaalde identiteit de jouwe is. Dit is een eeuwenoud probleem, waar verschillende oplossingen voor bedacht zijn. Vaak worden authenticatiemiddelen opgedeeld in: iets wat je *hebt*, iets wat je *weet*, iets wat je *bent*. Deze drie middelen zullen achtereenvolgens kort besproken worden.

Een typische vorm van een authenticatiemiddel dat is gebaseerd op bezit is een gewone sleutel. De achterliggende gedachte is dat iedereen die in het bezit is van een passende sleutel ook legitiem toegang heeft. Indien er bij een inbraak geen braakschade geconstateerd wordt zal een verzekeringsmaatschappij concluderen dat de dief een sleutel had en dus gerechtigd was om naar binnen te gaan. De maatschappij zal de schade dan niet vergoeden.

Authenticatie op basis van iets wat je bezit is natuurlijk niet zo sterk. Dit bezit kan gestolen worden, of gekopieerd. Het is slechts op een zwakke manier aan een persoon gebonden.

Een sterkere vorm van authenticatie vindt plaats op basis van iets wat je weet. Een voorbeeld is een wachtwoord, of een PIN. Ook hier is de gedachte dat iedereen die het juiste 'geheim' kent legitiem toegang heeft. Wanneer ik bij mijn bank klaag over een spookafschrijving, maar de bank kan aantonen dat de juiste PIN gebruikt is, sta ik heel erg zwak. De vertrouwelijkheid van mijn PIN is mijn eigen verantwoordelijkheid. Indien iemand anders mijn PIN weet zal de bank ervan uitgaan dat ik die persoon toestemming gegeven heb aan mijn rekening te komen. Banken zullen bij zo'n spookafschrijving met juiste PIN de schade niet vergoeden, tenzij er sprake blijkt te zijn van een patroon: wanneer er meerdere klachten zijn en alle klagers op een bepaalde plaats geweest zijn is het aannemelijk dat aldaar de PINs afgekeken zijn, bijvoorbeeld via een *skimmer* om de magneetstrip op de pas te lezen en via een kleine camera op een betaalautomaat voor de PIN.

Hiermee komen we bij het zwakke punt van authenticatie op basis van iets wat je weet: afkijken, of populair ook wel *shoulder surfing* genoemd. Dit is een bekend probleem. Het behoort inmiddels tot de e-etiquette om nadrukkelijk weg te kijken wanneer iemand anders zijn of haar wachtwoord intypt.

Een andere zwakte is dat iemand het geheim kan proberen te raden. Vooral computers zijn goed in het snel en systematisch raden van toegangscodes. Meestal gebruiken ze daarbij een woordenboek, zodat bekende woorden eerst geprobeerd worden. In dat geval spreekt men van een *dictionary attack*. Men kan natuurlijk het systeem beschermen door slechts drie pogingen toe te staan. Maar dat introduceert weer nieuwe nadelen: ik kan daarmee van iemand anders de toegang blokkeren door voor die persoon een aantal pogingen te wagen. Het werkt beter een steeds grotere vertraging te introduceren bij herhaalde pogingen. Een ander nadeel is dat mensen hun geheim nogal eens vergeten. En als er veel verschillende geheimen (zoals wachtwoorden) onthouden moeten worden schrijven mensen ze vaak op. Daarmee wordt iets wat je weet tot iets wat je hebt.

Authenticatie op basis van iets dat je bent verwijst naar biometrie. Daarbij worden bepaalde lichaamseigen kenmerken gebruikt als bewijs van identiteit. Te denken valt aan een vingerafdruk, een iriscan, een DNA-profiel, of ook gewoon een foto. Biometrie kan ook gebaseerd zijn op gedrag, zoals de manier waarop je jouw handtekening zet (hoeveel druk op de pen op welk moment) of de manier waarop je een bepaald melodietje roffelt. Zulke gedragsmatige vormen van biometrie kunnen moeilijker afgedwongen worden bij personen die niet mee willen werken.

Biometrie wordt steeds meer toegepast. Er bestaan grote verwachtingen. Misschien wel teveel. De nadelen van biometrie worden vaak over het hoofd gezien. Wanneer je je PIN kwijtraakt kun je naar de bank gaan en om een nieuwe vragen. Wanneer echter je irisscan gecompromitteerd raakt heb je een groot probleem, simpelweg omdat vervanging niet echt een optie is. Wanneer iedereen van jou biometrische informatie af wil nemen om je te authenticeren raakt die informatie wijd verspreid, waardoor het risico toeneemt dat iemand er oneigenlijk gebruik van maakt door zich als jou voor te doen, bijvoorbeeld via een vervalste vingerafdruk. Een dun vliesje met jouw patroon is snel gemaakt, en moeilijk te detecteren.

Diefstal van biometrie kan ook in fysieke vorm, en neemt dan snel dramatische vormen aan. De uitgestoken oogbal uit Dan Brown's *Bernini Mysterie* is een voorbeeld. Een ander voorbeeld is de afgesneden vinger van een Maleisische zakenman die dacht dat hij zijn dure Mercedes S-klasse met een vingerafdruklezer goed beveiligd had. Door biometrie als authenticatiemiddel te kiezen vergroot je ook het persoonlijke lichamelijke risico voor betrokkenen.

Een ander nadeel van biometrie is de foutmarge. Die verschilt erg per vorm van biometrie. Bij iriscans worden weinig fouten gemaakt, bij vingerafdrukken iets meer, en bij gelaatsfoto's al veel meer, alleen al om dat gezichten in de tijd veranderen, door veroudering of verandering van bijvoorbeeld haar of bril. Daarnaast kunnen biometrische systemen gefopt worden, zeker wanneer er geen controleur in de buurt is. De vlies over een vinger is al genoemd, maar een gezichtsfoto kan voor een camera gehouden worden, of een speciale contactlens met een aangepast patroon kan bij de scanner gedragen worden. Het kost moeite, maar het kan. Geen enkel systeem is waterdicht.

Meestal worden de bovengenoemde authenticatiemiddelen in een bepaalde combinatie gebruikt. Toegang tot je bankrekening vereist authenticatie met iets wat je hebt (je bankpas) en iets wat je weet (je PIN). Een paspoort zit in de categorieën 'iets wat je hebt' en 'iets wat je bent' (door de foto, en binnenkort ook de vingerafdrukken in een chip).

Hoofdstuk 5

Wie ben ik?

Tot nu toe is op een nogal luchtige wijze gesproken over identiteiten van personen. Maar waar hebben we het dan eigenlijk over? Het gaat me er niet om hier een diepgravende filosofische analyse uit te voeren met medeneming van psychologische randgevallen als meervoudige persoonlijkheden, maar meer om een intuitief werkbaar identiteitsbegrip te formuleren waarmee we in de digitale wereld vooruit kunnen.

De meesten van ons ervaren gedurende ons leven een notie van ‘zelf’ als centrum van alle activiteiten waarin we betrokken zijn. Dit zelfbegrip kent een redelijke mate van continuiteit, ook al zijn onze ervaringen en reacties daarop heel verschillend gedurende de loop van ons leven. Het feit dat we voortbouwen op onze eerdere ervaringen versterkt dit gevoel van ‘ik’. Maar tegelijkertijd zijn er grote verschillen tussen een persoon aan het begin en aan het eind van het leven.

Aan anderen zijn we geneigd eenzelfde zelfbegrip toe te kennen. Maar van buitenaf bezien, puur gedragsmatig, weten we daar niet veel van. We kennen en herkennen anderen via bepaalde attributen (eigenschappen), waarbij uiterlijke kenmerken een belangrijke rol spelen. Ook kunnen we onszelf via lichaamseigen of gedragsmatige attributen omschrijven: roodharig, impulsief, drammerig, wispelturig of charmant. Als benadering zouden we persoonlijke identiteit kunnen omschrijven als geheel van attributen waaraan we op dit moment voldoen. Identiteit is daarmee geen statisch gegeven: ik ervaar mezelf ook zeker niet als dezelfde persoon als dertig jaar geleden. Het is moeilijk aan te geven wat er werkelijk constant blijft gedurende een mensenleven. Je DNA? Dat lijkt te voldoen, maar het is (op dit moment in de geschiedenis) zeer twijfelachtig of mensen zich identificeren met hun DNA. Zijn er dan andere, werkbare, goed herkenbare, identificerende attributen?

Je kan je naam ook goed als attribuut zien. Je naam wordt mogelijk in een huwelijk aangepast, maar blijft verder constant—uitzonderingen daargelaten. Kan mijn naam dan niet als identificerend attribuut gezien worden? Dat kan in redelijke mate, maar er zijn twee fundamentele problemen.

Hoe onderscheidend zijn namen eigenlijk? Ons huidige (westerse) namenstelsel is ingevoerd onder Napoleon, en werkt redelijk op locale schaal. Maar niet op wereldschaal. Ik heb een collega aan de Universiteit van Leuven in België die ook Bart Jacobs

heet, en zelfs op een verwant vakgebied werkzaam is. We worden soms verwisseld. Je zou dus extra attributen moeten toevoegen, zoals geboortedatum, of adres (huis, email, web). Adressen zijn daarbij minder geschikt, omdat ze het nadeel hebben dat ze nogal eens kunnen veranderen. Je moet dan de historie bijhouden: Bart Jacobs, die nu woont op . . . , daarvoor op . . . , enzovoort. Dat is niet praktisch. De geboortedatum is stabieler, en wordt daarom veel gebruikt. Een ander nadeel van deze extra attributen is dat niet iedereen ze altijd prijs wil geven. Sommigen houden hun leeftijd het liefst verborgen—al was het alleen maar uit ijdelheid—en anderen houden hun adres geheim—uit veiligheidsoverwegingen of gewoon om niet lastig gevallen te worden. Naam, geboortedatum en adres zijn privacygevoelige gegevens, die van belang zijn voor de persoonlijke veiligheid. Een kwaadwillende kan er identiteitsroof mee plegen en veel schade mee berokkenen.

Iets praktischer dan een naam is een nummer. Op nationale schaal hebben we inmiddels zo'n systeem, waarbij iedereen een Burger Service Nummer (BSN) heeft. Dat werkt inderdaad als uniek identificerend—op nationale schaal. Ik identificeer mijzelf echter niet of nauwelijks met mijn BSN. Ik ken het niet eens uit mijn hoofd en wanneer iemand mijn BSN roept reageer ik niet. Het heeft vooral een administratieve functie voor de overheid.

Het andere probleem met namen is dat ze op zich niks zeggen: *what is in a name?* Aan iemand die ik niet ken kan ik me bekend maken als Piet Jacobs. In kleine omgeving komt zulk bedrog snel aan het licht, wanneer blijkt dat anderen mij bijvoorbeeld Klaas noemen. Maar op het internet kan het aannemen van een andere naam veel langer goed gaan.

Hoe kom je er nu achter dat Bart Jacobs mijn 'echte' naam is. Misschien is het wel een pseudoniem! Ik heb een eigen webpagina[1], die een koppeling legt tussen mijn naam en een foto. Dat geeft misschien enig vertrouwen. Maar de webpagina heb ik zelf gemaakt, en zou dus enkel kunnen dienen om een pseudoniem geloofwaardigheid te geven.

Als u werkelijk mijn naam zeker wil weten kunt u mij vragen mijn paspoort te tonen. Ervan uitgaande dat ik dat doe, bent u inderdaad een stapje verder. Het paspoort geeft een koppeling tussen een naam (plus geboortedatum, BSN enzovoort) en een foto. Vervolgens dient u zichzelf ervan te overtuigen dat ik inderdaad degene ben die op de foto staat, en dat het paspoort echt is. Als het goed is vormt het paspoort (of rijbewijs of nationale identiteitskaart) een authentiek (door bevoegde autoriteiten uitgegeven) en integer (echt, niet vervalst) identiteitsdocument.

Maar hoe betrouwbaar is zo'n identiteitsdocument? Fraude met de documenten zelf (zoals vervalsing) zal later uitgebreider aan bod komen (in Hoofdstuk 13). Hierbij gaat het me erom hoe het document tot stand komt. Het is gebaseerd op informatie in de gemeentelijke basisadministratie (GBA) van mijn woonplaats. Een goede vraag is hoe men daarin komt, en wanneer de koppeling met een foto plaatsvindt. Opname in de GBA vindt plaats vlak na de geboorte. Er wordt dan enkel een nieuwe naam met

[1] Namelijk `www.cs.ru.nl/B.Jacobs`

een geboortedatum, tezamen met de namen van de ouders opgenomen. De gemeente heeft in dat stadium nog geen manier om te weten om wie het werkelijk gaat[2].

Vorig jaar heb ik mijn kinderen in mijn paspoort bij laten schrijven. Toen vond feitelijk voor hen de eerste koppeling tussen naam en foto plaats. De daarbij gebruikte controle aan de balie van de burgelijke stand stelde echter helemaal niks voor, simpelweg omdat de gemeente niks in handen heeft om een deugdelijke controle uit te voeren. Mijn kinderen werd enkel gevraagd hoe ze heten en hoe oud ze waren. Vervolgens werden de pasfoto's die ik van ze meegenomen had vergeleken. Ik had net zo goed de kinderen van de buren mee kunnen nemen met passende foto's—plus de instructie om de namen en leeftijden te noemen die sinds de geboorteaangiften in de GBA staan. Ik heb de betreffende ambtenaar gevraagd of ze eigenlijk wel zeker wist dat dit mijn kinderen waren en niet die van een ander. Ze vertelde dat ze het inderdaad niet zeker kon weten, en gaf ook aan dat ze soms het gevoel had dat de zaken niet klopten. Het wordt algemeen erkend dat gemeentelijke basisadministraties behoorlijk wat onjuistheden bevatten. Daarmee zijn de op de GBA gebaseerde identiteitsdocumenten ook niet altijd betrouwbaar.

We stellen vast dat ons systeem van naamgeving historisch gegroeid is, een beperkte reikwijdte heeft en geen absoluut betrouwbare basis heeft. Het geheel functioneert desondanks redelijk vanwege de benodigde consistentie in verschillende contexten. Het systeem is in huidige vorm echter niet geschikt om online (op het web) de identiteit van de partij aan de andere kant van de lijn vast te stellen. Een paspoort voor een webcam houden geeft niet zo heel veel vertrouwen. Ook is het goed te beseffen dat alle beveiligings- en controle-mechanismen die gebaseerd worden op de huidige infrastructuur niet waterdicht zullen zijn.

Absolute zekerheid kan alleen via zeer vergaande maatregelen, zoals het direct koppelen van een BSN aan DNA bij geboorte. Dat vereist dat in de rest van de keten ofwel alle controles plaatsvinden op basis van DNA, ofwel dat DNA op enig later moment aan een andere vorm van biometrie gekoppeld wordt. Grootschalige DNA-controle is op dit moment echter geen optie, omdat het veel te veel tijd en geld kost. Daarnaast is DNA-analyse erg privacygevoelig omdat op basis van mijn DNA erfelijke ziektes vastgesteld kunnen worden. Verzekeringsmaatschappijen of hypotheekverstrekkers kunnen mogelijk oneigenlijk gebruik maken van zulke informatie. Koppeling aan een andere vorm van biometrie is wel een optie, maar kan pas na enkele jaren. Vingerafdrukken bijvoorbeeld zijn bij jongeren (en ouderen) niet erg betrouwbaar. Sowieso zal het een hele generatie duren voordat zo'n systeem met koppeling tussen BSN en DNA bij geboorte volledig doorgevoerd is.

[2] Er is in principe wel iets meer informatie voorhanden: na de geboorte wordt in Nederland bij bijna alle kinderen (toestemming van ouders is nodig) via een hielprik een druppeltje bloed afgenomen voor screening op aangeboren stofwisselingsziekten. Op dat moment komt natuurlijk DNA-materiaal beschikbaar, maar het is onduidelijk in hoeverre dit bloedmonster gekoppeld wordt aan een officieel geboortebewijs (met de naam). De bloedmonsters worden trouwens niet vernietigd, maar blijven bewaard bij het Rijksinstituut voor Volksgezondheid en Milieu (RIVM) te Bilthoven voor medisch-wetenschappelijk onderzoek.

Zo'n koppeling van BSN en DNA is alleen betrouwbaar op nationale (of mogelijk Europese) schaal. De identiteit van vreemdelingen uit verre landen kan er nog steeds niet mee vastgesteld worden. Uiteindelijk hebben we dus niet zoveel zekerheid over identiteiten.

Hoofdstuk 6

Rollen en privacy

Privacy is een gecompliceerd begrip, waar geen eenduidige omschrijving van te geven is. Er zijn omvangrijke en diepgaande juridische en filosofische studies die zich met het begrip bezighouden. Er is het klassieke werk van de Amerikaanse juristen Warren en Brandeis uit 1890 waarin gesproken wordt over *the right to be let alone* en privacy in het licht staat van ongewenste openbaarmaking en bemoeienis. De context werd destijds gegeven door de opkomst van de populaire pers met een voor die tijd nieuwe vorm van opdringerige journalistiek. Een andere lijn plaatst privacy in de context van individuele menselijke waardigheid, waarbij het gezien wordt als wezenlijke voorwaarde voor persoonlijke vrijheid en autonomie en voor de mogelijkheid om eigen, door anderen gerespecteerde keuzes te maken, waardoor de ruimte bestaat om af te wijken van de norm en eigen fouten te maken. Hieronder zullen we meer de nadruk leggen op de sociale aspecten van privacy als noodzakelijke voorwaarde om verschillende rollen en contacten te onderhouden. Dit volgt het werk van denkers als James Rachels en Ruth Gavinson.

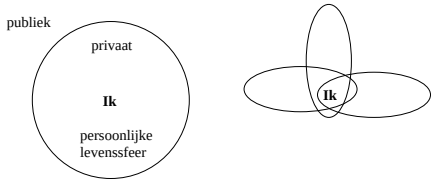
We hebben allemaal denk ik een redelijk intuitief begrip van privacy. Er schiet vast wel een situatie te binnen waarbij u zich ooit in uw privacy aangetast voelde, en waarbij u het gepast vond wanneer een ander het hoofd afgewend had, of helemaal niet aanwezig geweest was. Het gaat me om situaties waarvan een Engelsman droogjes opmerkt: *we don't talk about it.* Evengoed zijn er situaties voorstelbaar waarin u het ongepast of onheus of zelfs bedreigend vindt wanneer de staat of een bedrijf meekijkt. Wanneer het gaat om uw persoonlijke levenssfeer garandeert de grondwet (in artikel 10) dat die ongepastheid de vorm heeft van een recht op eerbiediging, om verschoond te blijven van zulk meekijken.

In ons leven spelen we veel verschillende rollen: bijvoorbeeld moeder, dochter, lid van de tennisclub, kerkganger, onderwijzer, vrijwilliger in de vluchtelingenhulp, suikerpatiënt en initiatiefnemer van een praatgroep voor misbruikte vrouwen. Bij ieder van die rollen hoort een bepaald verband, meestal kleinschalig, dat zin verschaft, en ook een bepaalde deel-identiteit met een eigen sfeer van vertrouwelijkheid. Doorbreking van die sfeer is in meer of mindere mate ongepast. Mensen hechten er in het algemeen aan zulke verschillende rollen gescheiden te houden. Soms expliciet,

maar ook heel vaak impliciet. Ze gedragen zich soms ook heel anders in verschillende rollen: de saaie kantoorklerk kan de grootste lolbroek zijn van de visclub. Zulke verschillen worden in het dagelijkse leven breed geaccepteerd. Ik heb er in principe niks mee te maken wat voor hobbies mijn baas heeft. Ik kan er belangstellend naar vragen, maar wanneer hij er weinig over wil vertellen accepteer ik dat. Als ik toch doorvraag is dat ongepast. Voor de (zakelijke) omgang die ik met mijn baas heb is kennis van zijn hobbies voor mij niet noodzakelijk.

Privacy is belangrijk juist omdat het zo'n scheiding van verschillende rollen mogelijk maakt. Privacy beschrijft het 'recht' om informatie tot een bepaalde rol te beperken. Privacy maakt het mogelijk dat verschillende mensen respectvol met elkaar samenleven en is dus essentieel in een pluriforme samenleving. Als ik zou weten dat mijn baas zijn vrouw slaat of bij de Bhagwan is zou ik misschien helemaal niet goed met hem samen kunnen werken.

Privacy is aldus een wezenlijk onderdeel van sociale interactie. Ons leven is gecompartimentaliseerd in verschillende rollen, en daar hoort een compartimentalisatie van informatie essentieel bij. De grondwet beschermt privacy in de formulering van eerbiediging van de persoonlijke levenssfeer. Traditioneel wordt er in discussies over privacy een onderscheid tussen publiek en privé gemaakt. Een passender en meer gedifferentieerde formulering, die hier gevolgd wordt, zou iedere levenssfeer of rol moeten beschermen, zoals in het onderstaande plaatje gesuggereerd wordt.



Traditionele tegenstelling

Differentiatie naar rollen

In het vervolg wordt uitgegaan van een intuïtief, niet nader omschreven, begrip van persoonlijke rol. We zullen daarbij de termen 'rol' en 'levenssfeer' als synomiem gebruiken, in algemene zin, en dus niet beperkt tot *persoonlijke* levenssfeer. Een rol/levenssfeer kan de omgang betreffen met je baas, met de vertrouwenspersoon van de afdeling personeelszaken, met je echtgenoot, met je maîtresse, met de pastoor, met de huisarts enzovoort. Het is een uitdaging om ook in de online wereld een formalisatie (als onderdeel van automatisering, zoals beschreven aan het begin van Hoofdstuk 4) van deze opvatting van rol als (gedeeltelijk) afgescheiden levenssfeer te vinden. Door zo'n gedifferentieerde formalisatie sluit ICT aan bij dagelijkse sociale praktijken, door juist niet de nadruk te leggen op afgedwongen uniformiteit. Op wat daar voor nodig is zal het volgende hoofdstuk nader ingaan.

Voor het gescheiden houden van de diverse rollen die we spelen is het wezenlijk dat we zelf een redelijke mate van controle hebben over wie toegang heeft tot (welke

informatie over) ons. Privacy betreft aldus 'informationele zelbeschikking', niet alleen met betrekking tot de vraag wanneer je aan wie informatie over jezelf weggeeft, maar ook wat er vervolgens mee gedaan wordt. Dit tweede aspect wordt nader besproken in Hoofdstuk 12 in termen van *policies* als gebruiksbeslissingen.

In het intermenselijke verkeer is privacy nodig bij de opbouw van onderling vertrouwen, typisch in kleinschalige verbanden, via *selective self-disclosure* waarbij vertrouwelijke informatie die bij een rol/levenssfeer hoort onderling gedeeld wordt. De partijen worden geacht deze vertrouwelijkheid te handhaven. Zo niet, dan is er sprake van een vertrouwensbreuk. Afgedwongen openheid en doorbreking van rollen via monitoring, data surveillance en profilering is onnatuurlijk—en bruuskerend, of zelfs vernederend—want vindt plaats buiten een kader van onderlinge vertrouwensopbouw en gelijkwaardigheid.

Het uit elkaar houden van onze verschillende rollen kost enige moeite, maar is op zodanige manier ingesleten in onze sociale patronen dat we ons er vaak nauwelijks expliciet bewust van zijn. Maar soms is het ook goed zichtbaar, bijvoorbeeld wanneer iemand verschillende mobiele telefoons gebruikt, ieder voor een eigen rol. Ervaring van vrijheid en autonomie is, meen ik, sterk gekoppeld aan de mogelijkheid om zelf nieuwe rollen te kiezen en zelf de bij die rollen horende informatie te beheren en al of niet gescheiden te houden.

Privacybescherming

Er wordt soms lukraak beweerd dat mensen niet meer aan privacy hechten. Indien privacy in bovenstaande zin verstaan wordt kan ik me dat nauwelijks voorstellen. Er zijn onderlinge verschillen tussen mensen in de mate waarin ze hun rollen door elkaar laten lopen, maar volstrekte transparantie tussen al hun rollen is volgens mij erg ongebruikelijk. Privacy is als zuurstof nodig voor het draaiend houden van het intermenselijke verkeer en het vormt de grondslag voor onderlinge banden gebaseerd op vertrouwen.

Indien we onze ICT-infrastructuur op welke manier dan ook een menselijk gezicht willen geven zal privacybescherming daar een wezenlijk onderdeel van moeten zijn. De structuur zal mensen op een soepele, intuitieve manier de mogelijkheid moeten bieden om ook online verschillende rollen te spelen—en uit elkaar te houden! Idealiter zou dit compartimentaliseren van rollen online net zo moeiteloos moeten verlopen als we offline gewend zijn. Het koppelen van informatie uit verschillende domeinen moet daarbij met de grootst mogelijk terughoudendheid gebeuren omdat er mogelijk (gegevens uit) rollen gekoppeld worden die betrokkenen gescheiden wensen te houden.

Hoe we die rollen online praktisch het beste uit elkaar kunnen en willen houden vormt een grote uitdaging. Individuele *policies* kunnen daarbij een rol spelen. Maar een eerste stap is erkenning van de individuele pluriformiteit. Iedereen altijd uniform op dezelfde wijze benaderen, zoals via het Burger Service Nummer (BSN), gaat in volstrekt tegengestelde richting. Ook tegenover de overheid (en al de andere instanties die het BSN gebruiken) spelen mensen verschillende rollen.

Bedrijven en overheden die grootschalige gegevens van individuen opslaan eisen

een bepaalde vertrouwensband op die misschien volkomen ongepast en misplaatst is. Vertrouwen wordt je geschonken en hoor je te verdienen, en kan zeker niet eenzijdig afgedwongen worden. Omdat het delen van gevoelige informatie zo wezenlijk is voor het sociale proces van vertrouwensopbouw in een relatie zou hier omzichtiger mee omgegaan dienen te worden. De menselijke maat is ermee gediend indien er beter nagedacht zou worden over het eigen gedecentraliseerde beheer van gegevens die bij een specifieke rol horen[1].

Meerdere identiteiten

Nu we op dit punt aangekomen zijn is duidelijk dat de vraag “wie ben ik” uit Hoofdstuk 5 geen eenduidig maar een gedifferentieerd antwoord heeft. Het hangt helemaal af van mijn rol. Bij ieder van mijn rollen hoort een eigen deel-identiteit of rol-identiteit, bepaald door de attributen die in die rol op mij van toepassing zijn. Bij sommige van die rollen speelt mijn naam een rol—bijvoorbeeld als patiënt bij de huisarts—maar sommige rollen zijn anoniem—bijvoorbeeld als koper van een rol WC-papier (als ik kontant betaal, tenminste). Sommige rollen zijn tijdelijk, met een bijbehorende tijdelijke identiteit, zoals houder van een geldig garantiebewijs op een strijkijzer, of bezoeker van een pornofilm. Daarvoor is mijn naam niet nodig.

Ook online zouden we de zaken zo willen organiseren dat mensen over verschillende (mogelijk tijdelijke) identiteiten kunnen beschikken. Gedeeltelijk werkt het natuurlijk al zo. Ik heb bijvoorbeeld aanstellingen aan twee universiteiten, namelijk in Nijmegen en Eindhoven. Ik heb daar verschillende emailadressen die ik strikt gescheiden probeer te houden: één voor Nijmeegse en één voor Eindhovense zaken. Op zo’n manier is altijd duidelijk vanuit welke rol (met welke pet) ik een email schrijf. Ook beperk ik bepaalde informatie tot slechts één van die twee aanstellingen. Voor iedere tijdelijke rol zou ik een nieuw (hotmail of gmail of ander) adres kunnen gebruiken. Dat is een beetje omslachtig en kan ook anders.

[1] Ook vanuit andere perspectieven is er groeiend verzet tegen onpersoonlijke en uniforme grootschaligheid, zie bijvoorbeeld Ad Verbrugge’s *Tijd van Onbehagen* (SUN, Nijmegen, 2004).

Deel III

Beheer van Identiteiten

Hoofdstuk 7

Versleuteling

Soms willen mensen elkaar berichten of brieven sturen zonder dat iemand anders de inhoud lezen kan. Traditioneel willen diplomaten, militairen en spionnen dat, maar bijvoorbeeld ook veel geliefden. Ook bedrijven willen soms bepaalde boodschappen of gegevens verhullen, bijvoorbeeld wanneer sprake is van concurrentie- of beurs-gevoelige inhoud. En binnen de overheid of gezondheidszorg zou je verwachten dat staatsgeheimen en privacygevoelige gegevens van burgers niet zomaar toegankelijk zijn. Het willen kunnen verbergen van bepaalde inhoud is een volkomen normale en gerechtvaardigde wens.

Je zou mischien denken: als je een geheim bericht te versturen hebt dan schrijf je het niet op een briefkaart, maar stop je het toch in een enveloppe. Er bestaat weliswaar een wettelijk vastgelegd briefgeheim, maar erg veel bescherming biedt dat niet, want iedere kwaadwillende kan de enveloppe openscheuren. Een iets betere beveiliging wordt geboden door met een sleutel afsluitbare kistjes. Wanneer beide partijen een sleutel hebben kunnen ze onderling afgesloten kistjes heen en weer sturen. Helemaal waterdicht is dit nog niet, want ook de kistjes zouden opengebroken kunnen worden—met geweld of via een loper. Maar fysieke afscherming is in veel situaties een goed beveiligingsmechanisme.

Er zijn echter slimmere manieren om zoiets te doen, zonder dat er fysieke kistjes en sloten aan te pas hoeven te komen. De Romeinse veldheer Julius Caesar had al zo'n truuk. Wanneer hij een geheim bericht naar een van zijn generaals wilde sturen schreef hij het bericht eerst op papier, en verplaatste daarna alle individuele letters in het bericht drie posities naar achter in het alfabet. Het bericht

> obelix is weer actief

wordt dan

> rehola lv zhhu dfwlhi

Het resultaat werd door een koerier bezorgd. Wanneer dit gecodeerde bericht onderweg onderschept werd gingen er geen geheimen verloren, want Caesar ging er van

uit dat zijn tegenstanders—degenen die konden lezen—niet slim genoeg waren om de versleuteling te doorbreken.

Terzijde: deze vorm van versleuteling door verwisseling van letters is naar moderne maatstaven zeer zwak. De verwisselmethode kan snel herkend worden aan de hand van de frequentie van letters. Daar zijn lijsten van. De ‘e’ is bijvoorbeeld de meest voorkomende letter in het Nederlands. In de bovenstaande versleutelde tekst ‘rehola lv zhhu dfwlhi’ komt de ‘h’ het meeste voor, namelijk vier keer. Men kan er—in dit geval terecht—van uitgaan dat die letter overeenkomt met de ‘e’. Met een beetje puzzelen kom je er dan snel uit. Zulk gepuzzel spreekt veel mensen aan, net als sudoku’s of cryptogrammen.

Cryptografie is de wiskundige discipline die zich bezighoudt met het versleutelen van boodschappen. Er zijn tegenwoordige slimme versleutelingstechnieken die door computers razendsnel uitgevoerd kunnen worden. Ze zijn praktisch niet te kraken, niet door mensen en ook niet door computers, ook al kunnen die bijvoorbeeld heel snel heel veel mogelijkheden uitproberen.

Bij zo’n wiskundige versleuteling is meestal sprake van een methode—zoals: verschuif letters in het alfabet naar achter—en een sleutel—zoals: drie posities. Zo’n sleutel is in de moderne praktijk meestal een heel groot getal. De methode mag best bekend zijn, maar de sleutel moet geheim blijven[1]. Wanneer nu twee partijen van te voren een methode en een geheime sleutel afgesproken hebben, dan kunnen ze daarmee onderling geheime boodschappen uitwisselen—net als Caesar deed, en net alsof ze de berichten verpakt hadden in afgesloten kistjes.

Zulke versleuteling vormt de klassieke basis voor beveiligde communicatie. Maar je kunt de techniek ook gebruiken voor beveiligde opslag. Wanneer je militaire geheimen eerst versleutelt voor je ze op een memory stick zet is het niet zo erg wanneer je die stick verliest. De vinder kan de versleutelde gegevens toch niet lezen, zolang jij je sleutel maar geheim houdt, en zeker niet ook op de memory stick zelf zet. Dat laatste is dom, en is vergelijkbaar met het hangen van een huissleutel aan de deurbel. Je hoeft bij versleutelde opslag de sleutel ook helemaal niet met iemand anders te delen: het is voldoende dat jij weet wat die sleutel is, zodat je daarmee weer kunt ontsleutelen op het moment dat je de gegevens van je eigen stick nodig hebt. Wanneer je de memory stick voor overdracht (communicatie) gebruikt moet je de sleutel natuurlijk wel delen zodat de andere partij kan ontsleutelen.

In het digitale tijdperk zullen we moeten leren omgaan met zulke digitale sleutels. Die sleutels zijn getallen, die in feite zo groot zijn (wel tientallen tot honderden cijfers) dat we ze onmogelijk kunnen onthouden. Hoe moeten we ze dan beheren? Er zijn ruwweg twee methoden.

In het eerste geval staat de geheime sleutel op je computer, maar is alleen toegankelijk via een wachtwoord. Een speciaal programma zorgt er dan voor dat je bij versleuteling of ontsleuteling van documenten alleen dat wachtwoord in hoeft te typen. Met de sleutel zelf heb je in feite niet direct te maken.

[1] Dit staat bekend als het principe van Kerckhoffs, reeds geformuleerd in 1883.

In het tweede geval staat de geheime sleutel op een aparte chipkaart, die je in (een kaartlezer bij) je computer moet steken om te versleutelen of te ontsleutelen. Die chipkaart kan vervolgens beveiligd worden met een PIN. Het voordeel hiervan is dat je jouw sleutel(s) makkelijk met je mee kan nemen. Een SIM-kaartje in een mobiele telefoon is hiervan een voorbeeld. De SIM is een als chipkaart, maar dan alleen de chip zonder plastic kaartje eromheen. De SIM wordt geactiveerd door een PIN, en bevat de cryptografische sleutels waarmee jouw telefoongesprekken vercijferd worden. De gesprekssignalen van een mobiele telefoon kunnen weliswaar met een speciale ontvanger uit de lucht geplukt worden, maar zijn niet zomaar af te spelen. Zulke handige beveiligde mobieltjes had Caesar graag gehad.

Hoofdstuk 8

Digitale handtekeningen

Bij de ‘klassieke’ manier van versleutelen uit het vorige hoofdstuk hebben partijen één gedeelde geheime sleutel voor de onderlinge communicatie. Sinds eind jaren zeventig van de vorige eeuw bestaat er een opmerkelijke techniek die veel krachtiger is: zogenaamde publieke cryptografie. Daarbij heeft iedere partij een tweetal (gekoppelde) sleutels, eentje geheim, en eentje publiek. De publieke sleutel is inderdaad bedoeld om openbaar te maken, bijvoorbeeld in een speciaal telefoonboek. Op mijn persoonlijke webpagina staat bijvoorbeeld mijn publieke sleutel[1].

Wat kun je zoal doen met zo’n sleutelpaar? Dat zijn verschillende dingen, voor verschillende doeleinden. Daar zit dan ook de kracht. Voor het gemak zal ik mijn sleutelpaar een naam geven, namelijk pub_{bj}, priv_{bj}, waarbij de naam al suggereert dat pub_{bj} mijn publieke en priv_{bj} mijn geheime sleutel is. Deze twee sleutels horen bij elkaar, omdat er twee kanten op mee versleuteld en ontsleuteld kan worden, waardoor er samen de volgende handige zaken mee te doen zijn.

1. **Vertrouwelijke berichten sturen.** Indien u mij een boodschap wil sturen die niemand anders mag zien, dan haalt u eerst mijn publieke sleutel pub_{bj} van mijn webpagina en versleutelt u vervolgens die boodschap met pub_{bj}. Daarna kunt u het versleutelde resultaat op welke onbeveiligde manier dan ook naar mij toesturen: gewoon per email, op de achterkant van een postkaart, of via een nieuwsgierige koerier. Voor de ontsleuteling is namelijk de bijbehorende geheime sleutel priv_{bj} nodig—die ik alleen heb en die ik natuurlijk angstvallig geheim houd.

   Als ik u ook weer vertrouwelijk wil antwoorden dan versleutel ik mijn reactie met uw publieke sleutel. Alleen u kunt dan de vereiste geheime sleutel gebruiken om mijn bericht leesbaar te maken.

   Deze versleuteling met publieke cryptografie kan ook begrepen worden in termen van afsluitbare kistjes. Mijn publieke sleutel is dan een kistje met een hangslot dat gewoon dichtgeklikt kan worden, waarbij ik degene ben die als enige de

[1] Voor de cognoscienti: mijn publieke PGP sleutel is ook te vinden via de *KeyId* 576B9C3F. Nuttig voor zeer vertrouwelijke feedback.

geheime ‘privé’ sleutel bezit waarmee het hangslot geopend kan worden. Wanneer ik gratis kistjes met openhangende sloten ter beschikking stel en verspreid kan iedereen mij geheime berichten versturen, die ik alleen weer toegankelijk kan maken. Men hoeft alleen een zo’n ‘publiek’ kistje van mij te bemachtigen, te vullen, dicht te klikken, en naar mij op te sturen. Zelfs de verzender kan na ‘versleuteling’ niet meer bij het eigen bericht. Bij een gedeelde sleutel, zoals in het vorige hoofdstuk besproken, is dat nog wel mogelijk.

2. **Handtekening zetten.** Bij transacties zijn handtekeningen essentieel om aan te geven dat de ondertekenaar instaat voor het ondertekende document. Door een handtekening te zetten commiteer je je ergens aan en kan de andere partij je daar aan houden. Het moet daarbij duidelijk zijn dat het commitment echt van jou afkomstig is, waardoor er iets van jou alleen voor nodig is. In digitale vorm wordt daarvoor de geheime sleutel priv_{bj} gebruikt.

   Stel ik wil mijn bank een digitale opdracht geven om aandelen Microsoft te kopen. De bank accepteert alleen ondertekende opdrachten van klanten, en daarom onderteken ik de opdracht met mijn geheime sleutel priv_{bj}. Die ondertekening is in feite ook weer een apart soort versleuteling. De bank weet mijn publieke sleutel pub_{bj} en kan daarmee het bericht ontsleutelen en de handtekening controleren. Het cruciale punt is dat de bank nu weet dat het bericht echt van mij afkomstig is omdat alleen degene die de sleutel priv_{bj} heeft iets kan versturen dat met pub_{bj} herkend kan worden.

   De volgende dag wint eindelijk iemand een rechtszaak waarin Microsoft verantwoordelijk wordt gehouden voor de vele fouten in zijn software. De beurskoers van het bedrijf keldert als gevolg. Ik probeer tegenover mijn bank te ontkennen dat ik aandelen besteld heb. Ook daar komt een rechtszaak over. Mijn bank toont de rechter de met priv_{bj} ondertekende opdracht, die de rechter zelf met mijn publieke sleutel kan controleren. Volgens Europese (en inmiddels ook Nederlandse) wetgeving hebben digitale handtekeningen dezelfde juridische status als gewone handtekeningen[2]. Ik sta in mijn hemd, verlies het proces en zit alsnog met de aandelen opgescheept (en waarschijnlijk ook met een rekening voor de proceskosten). Deze geheime sleutel priv_{bj} functioneert dus als een PIN en zorgt voor de zogenaamde onloochenbaarheid die essentieel hoort bij handtekeningen.

   De elektronische handtekening is als een “omgekeerd slot” op een doosje: alleen ik kan het slot erop doen (met mijn geheime sleutel), maar iedereen kan het vervolgens openenen (met mijn publieke sleutel).

   De digitale handtekening kan goed gecombineerd worden met vertrouwelijke communicatie uit het vorige punt. Stel u wil mij een vertrouwelijk contract sturen. U versleutelt het contract dan eerst met uw eigen geheime sleutel, en vervolgens met mijn publieke sleutel. Ik kan—en niemand anders—de boel dan ontsleutelen met mijn eigen geheime sleutel, en uw handtekening controleren met uw publieke sleutel. U heeft zich tegenover mij gecommiteerd, maar niemand weet ervan. Prachtig toch!

3. **Authenticatie: bewijzen wie je bent.** Stel u heeft een eigen bedrijf met in de kelder een zeer geheime ruimte waartoe maar een beperkt aantal mensen toegang hebben. Van al die mensen kent u de identiteit en de publieke sleutel. U zet nu bij de keldertrap een speciaal elektronisch poortje met klapdeuren dat de identiteit van mensen die de kelder in willen moet controleren. Stel ik sta op de lijst van mensen die toegang hebben tot de kelder. Wanneer ik de trap af kom is het poortje dicht, en vraagt het aan mij wie ik ben. Ik identificeer mij door mijn naam te zeggen, waarbij het poortje denkt: “ja, ja, zo willen we allemaal wel heten”. Vervolgens geeft het poortje mij een zogenaamde *challenge*. Dat is een willekeurig bericht dat ik moet ondertekenen door het bericht te versleutelen met mijn geheime sleutel priv_{bj}. Dit is mijn *response*. Vervolgens controleert het poortje de handtekening met mijn (bekende) publieke sleutel pub_{bj}. Wanneer daarbij de oorspronkelijke *challenge* weer te voorschijn komt weet het systeem dat ik het ben en gaat het poortje open zodat ik door kan lopen. Ik ben immers de enige die priv_{bj} bezit en daarmee de challenge digitaal kan ondertekenen.

   In zulke *challenge-response* systemen is het van wezenlijk belang dat de *challenge* een willekeurig bericht is dat iedere keer anders is. Zou het namelijk iedere keer dezelfde vraag zijn dan kan een kwaadwillende mijn (ondertekende) antwoord een keer opvangen en de volgende keer afspelen zodat hij zich als mij kan voordoen.

   Een ander technisch punt is dat de functies 2 (handtekening) en 3 (authenticatie) zich niet laten combineren bij hetzelfde sleutelpaar. Bij de handtekening ben ik immers degene die het bericht kiest dat ondertekend wordt. Bij authenticatie kiest de omgeving de *challenge* en moet ik die ondertekenen, wat het ook is. Wanneer je 2 en 3 combineert kun je als omgeving een voor mij ongunstig contract als challenge opsturen. Ik onderteken het als *response* en ben daarmee gebonden aan iets wat ik niet wil. De oplossing is om voor handtekening en authenticatie verschillende sleutelparen te gebruiken.

[2] Daarbij moet wel aan een aantal kwaliteitseisen voldaan zijn.

Publieke cryptografie is dus een krachtig mechanisme, met vele mogelijkheden in de digitale wereld. Daar zullen we verder in het hoofdstuk nader op ingaan. Het is hier echter wel enigszins rooskleurig beschreven. Er zijn een aantal belangrijke issues bij betrokken die het grootschalige gebruik enigszins bemoeilijken.

Hoe weet iemand anders eigenlijk zeker wat mijn publieke sleutel is? Van die zekerheid hangt namelijk het hele systeem af. Ik heb het zo beschreven dat mijn publieke sleutel op mijn persoonlijke webpagina staat. Maar die webpagina heb ik zelf gemaakt, en geeft dus geen enkele garantie. Ik had er net zo goed de publieke sleutel van de koningin neer kunnen zetten (alsof het de mijne was), zodat het lijkt alsof dat wat zij ondertekent van mij afkomstig is (of andersom).

Het moge duidelijk zijn dat er een bevoegde autoriteit (bijvoorbeeld mijn gemeente) nodig is die moet verklaren: “de publieke sleutel van Bart Jacobs is pub_{bj}”. In de moderne wereld wordt die uitspraak natuurlijk zelf ook weer digitaal ondertekend met de geheime sleutel van de autoriteit (mijn gemeente). Het resultaat wordt een ‘certificaat’ genoemd. Het is iets preciezer om van ‘identiteitscertificaat’ te spreken omdat een identiteit aan een publieke sleutel gekoppeld wordt. Later zullen we nog andere soorten certificaten tegenkomen, namelijk met attributen in plaats van identiteiten.

Hiermee hebben we het probleem verplaatst, maar wel gereduceerd: om van alle bij Nederlandse gemeentes ingeschreven personen zekerheid te hebben over hun publieke sleutels hoef je alleen maar zekerheid te hebben over de publieke sleutels van alle gemeentes—ervan uitgaande dat je de gemeentes en hun procedures vertrouwt. Nu gaan we gewoon nog een stap hoger. We hebben ondertekende verklaringen (certificaten) nodig van de vorm “gemeente X heeft publieke sleutel pub_X”, want daarmee is de ondertekende verklaring over mijn publieke sleutel te controleren. Zulke verklaringen over de publieke sleutels van gemeentes worden dan weer ondertekend door het rijk, met geheime sleutel priv_{rijk}. Om die verklaring van het rijk te controleren hoef ik dus alleen nog maar te weten wat de bijbehorende publieke sleutel pub_{rijk} is. De zaak is is via een getrapte vertrouwensketen gereduceerd tot kennis van één sleutel, namelijk pub_{rijk}. Die ene publieke sleutel zou breed gepubliceerd kunnen worden, bijvoorbeeld in de Staatscourant en op allerlei webpagina’s van de overheid.

Het tweede probleem is dat mensen (en organisaties) soms slordig omgaan met hun geheime sleutel, of dat sleutels soms ingetrokken moeten worden, bijvoorbeeld bij beëindiging van een dienstverband. Wanneer mijn geheime sleutel bekend raakt kan iedereen in mijn naam handtekeningen gaan zetten. Op zo’n moment wil ik een nieuw sleutelpaar hebben en wil ik ook kunnen aangeven dat mijn oude sleutelpaar niet meer geldig is. Dat kan via zogenaamde *revocation lists* die eigenlijk altijd eerst gecheckt zouden moeten worden wanneer je een handtekening van een ander controleert. Zulke lijsten moeten beheerd worden door dezelfde bevoegde instanties die certificaten uitgeven. Het kan ook door certificaten slechts een korte geldigheid te geven. Hoe dat allemaal precies werkt voert hier iets te ver.

Gebruik van digitale handtekeningen

Misschien beziet u vooralsnog al die digitale handtekeningen als een ver-van-mijn-bed-show. Maar ze zijn dichterbij dan u denkt. De meesten van ons maken er zelfs al dagelijks gebruik van, niet direct in de vorm van het zelf zetten van een digitale handtekening, maar wel in de vorm van het controleren ervan.

Wanneer u op het internet surft verschijnen sommige pagina’s als ‘beveiligd’, zoals te zien is aan een gesloten slotje 🔒 ergens onder in een balk van uw webbrowser. Zulke beveiligde pagina’s worden typisch gebruikt voor meer gevoelige zaken, zoals het invullen van wachtwoorden en formulieren, of internetbankieren. Stel u bankiert online bij de Postbank, via de webpagina `http://mijn.postbank.nl`. Het gesloten slotje geeft dan aan dat er een certificaat gecontroleerd is dat iets zegt als: “het webadres `http://mijn.postbank.nl` is eigendom van de Postbank N.V.” Dit is goed om te weten zodat u uw bankgegevens niet invult bij een site van iemand anders. U zou daartoe verleid kunnen worden door een kwaadaardige zogenaamde *phishing* email die u naar een vrijwel identieke webpagina lokt op een ander adres. Indien u daar nietsvermoedend uw toegangscodes intikt kan vervolgens uw rekening geplunderd worden.

U kunt zulke certificaten ook zelf bekijken, typisch door op het gesloten slotje te klikken. Als u de gebruikte cryptografische operaties kent kunt u de gebruikte handtekening in principe ook zelf controleren. Maar gelukkig controleert ook uw webbrowser de handtekening op de uitspraak “het webadres `http://mijn.postbank.nl` is eigendom van de Postbank”. Maar welke partij heeft die handtekening dan gezet, en hoe weet ik dat die partij betrouwbaar is? Dat zijn zeer terechte vragen. Voor de webstek van de Postbank is de handtekening gezet door het bedrijf Thawte. Maar bijna niemand kent Thawte. Waarom zouden we Thawte eigenlijk vertrouwen?

Thawte is een zogenaamde *trust provider* die geld verdient aan het ondertekenen van documenten, zie `www.thawte.com`. Het is een soort elektronische notaris, die er op de lange termijn alle belang bij heeft om betrouwbaar te handelen. Mensen van de Postbank zijn daarnaartoe gegaan en hebben Thawte er op een of andere manier van overtuigd dat ze echt van de Postbank zijn en dat de website `http://mijn.postbank.nl` echt van hun is. Thawte heeft die uitspraak vervolgens ondertekend (met een geldigheid van ongeveer een jaar). Dit levert een certificaat. Dat certificaat wordt door de webpagina `http://mijn.postbank.nl` aan uw browser gegeven, die de handtekening controleert.

Maar hoe weet uw browser nu wat de bijbehorende publieke sleutel pub_{thawte} van Thawte is? Die is immers nodig om de handtekening, gezet met de bijbehorende geheime sleutel priv_{thawte}, te kunnen controleren, net zoals de eerdergenoemde publieke sleutel pub_{rijk} nodig is om gemeente-certificaten te controleren. De publieke sleutel pub_{thawte} blijkt al ingebakken te zitten in uw browser! De producent van uw browser heeft kennelijk al besloten dat Thawte te vertrouwen is, en dat alles wat Thawte ondertekent ook klopt. Dat gaat behoorlijk ver, maar zo is het nu eenmaal opgezet.

U heeft hier zelf nog wel enige controle over als u wil. Iedere gebruiker kan de publieke sleutels die ingebakken zitten in de eigen browser bekijken, en eventueel aanpassen. U kunt bijvoorbeeld een aantal publieke sleutels van organisaties die u zelf niet vertrouwt verwijderen, en andere toevoegen die u wel vertrouwt. Het is wel aardig daar eens naar te kijken in uw browser (zoek ergens onder ‘options’ of ‘preferences’ naar ‘certificates’). Zo is in de browser *Firefox* ook een publieke sleutel opgenomen van de Staat der Nederlanden. Daar heeft men bij *Firefox* kennelijk alle vertrouwen in.

Het getrapte controlemechanisme voor elektronische handtekeningen is de essentie van zogenaamde *Public Key Infrastructures* (PKIs). De term PKI kom je veel tegen in deze context.

In Nederland worden digitale handtekeningen bijvoorbeeld gebruikt door notarissen. De organisatie DigiNotar, zie `www.diginotar.nl`, verzorgt daarvoor de infrastructuur. Hiermee kan een aangesloten notaris ondertekende elektronische documenten bijvoorbeeld naar het kadaster sturen. Het kadaster controleert de digitale

handtekening met de publieke sleutel van de notaris. Deze digitalisering vergroot de efficiëntie—en waarschijnlijk ook de betrouwbaarheid en de veiligheid.

De Nederlandse overheid heeft een eigen initiatief, PKIoverheid genaamd, om het gebruik van digitale handtekeningen te stimuleren. Er wordt gewerkt aan een elektronische identiteitskaart met chip voor burgers met daarop een certificaat om digitale handtekeningen te zetten. Het certificaat zegt iets als "burger X met BSN Y heeft publieke sleutel Z". Deze bewering is dan voorzien van een elektronische handtekening door de Nederlandse Staat. Goed opgeborgen in de chip zit de geheime sleutel horend bij publieke sleutel Z. Daarmee kan burger X (met BSN Y) digitale handtekeningen zetten, bijvoorbeeld op persoonlijke aanvragen die X bij de gemeente of bij het rijk indient.

Internationaal zijn er ook 'open' initiatieven om certificaten uit te geven via persoonlijke netwerken van onderling bekenden, in plaats van via bedrijven zoals Thawte, zie bijvoorbeeld `www.cacert.nl`. Als je daar aan mee wil doen moet je eerst op zoek naar iemand die al meedoet en voor jou in wil staan. Op zo'n manier wordt een *web of trust* gecreëerd.

Een sleutelpaar, en handtekening, per rol

Veel mensen hebben verschillende email adressen, bijvoorbeeld één van het werk voor zakelijk gebruik en één voor privé gebruik. Daarmee kan op een snelle manier duidelijk gemaakt worden met welke pet op het hoofd een email geschreven wordt. Ik ken echter niemand die ook twee verschillende (gewone, handgeschreven) handtekeningen heeft. Toch zou het niet onlogisch zijn om onder een werkopdracht een andere handtekening te zetten dan onder een aanvraag voor zeg een nieuw paspoort of een vergunning voor uitbouw van het eigen huis. Dan zou ook in dat geval duidelijker zijn met welke pet op je je commiteert. Het lijkt mij overigens dat iedereen zich er bij het ondertekenen op een of ander niveau wel van bewust is of de eigen handtekening 'zakelijk' gebruikt wordt, of puur 'privé', of als secretaris van de locale paddenclub, of in welke rol dan ook.

Een van de aardige aspecten van digitale handtekening is dat je dat onderscheid heel goed kunt maken. Je hebt er simpelweg verschillende sleutelparen voor nodig: één voor op het werk, en één als ouder, en mogelijk nog één zeg als bezorgde (mogelijk anonieme) inwoner van je eigen stad voor het ondertekenen van petities. In feite kun je zo veel sleutelparen verzamelen als je wil: één voor iedere rol die je voor jezelf bedenkt. Je kunt voor ieder sleutelpaar/rol/levenssfeer dan een aparte chipkaart gebruiken. Als dit gebruik van meerdere handtekeningen breder ingeburgerd raakt verschijnen er ongetwijfeld handige apparaatjes of programmaatjes (bijvoorbeeld voor handcomputers of multifunctionele GSMs) waarmee je eenvoudig kunt selecteren welke handtekening in een bepaalde situatie gezet moet worden.

Is dit gebruik van meerdere handtekeningen lastig, of juist niet? Het lijkt mij wel handig en verhelderend, maar ook iets waar we even aan moeten wennen, net zo als we even moeten wennen aan het gebruik van meerdere email adressen of meerdere GSMs—voor werk of privé, of voor bellen met ouders of met vrienden. Vooral dat laatste onderscheid kan heel verschillende rollen en gedragingen betreffen. Zulke afbakeningen scheppen duidelijkheid en stellen je in staat om verschillende rollen met technische middelen te scheiden. Door de bijbehorende versleutelingsmogelijkheden kun je de verschillende gegevens die bij je verschillende levenssferen/rollen/sleutelparen horen ieder op een eigen manier versleutelen. Dit komt de privacy—in de vorm van het scheiden van rollen en gegevens—ten goede. Door deze nauwe koppeling tussen rollen en sleutelparen bestaat zelfs de neiging de twee te identificeren.

Hier zien we een voorbeeld waar moderne ICT kan bijdragen aan pluriformiteit, en ook standaard sociale patronen (meerdere gescheiden rollen per persoon, zie Hoofdstuk 6) kan ondersteunen. Techniek hoeft niet alleen uniformiserend en controlerend te werken. Maar dan moeten we die mogelijkheden wel herkennen, willen realiseren en ons enigszins willen inspannen om ze ons eigen te maken.

We zijn er allemaal redelijk van overtuigd dat er technisch veel mogelijk is om mensen in de gaten te houden. Maar er zijn ook veel technische (cryptografische) mogelijkheden om identiteiten te beschermen. Zo zijn er allerlei variaties van digitale handtekeningen, zoals:

- 'Blinde handtekeningen', waarbij een autoriteit een digitale handtekening zet zonder te weten waaronder. Dat is vergelijkbaar met iets bij een notaris in verzekerde bewaring afgeven zonder dat de notaris weet wat het is. Zulke handtekening worden bijvoorbeeld gebruikt voor anoniem digitaal geld, waarbij een bank een digitaal genummerd biljet ondertekent zonder het nummer te kennen—en dus zonder het gebruik ervan te kunnen volgen.

- 'Groepshandtekeningen', waarbij er één publieke sleutel kan dienen voor een groep van mensen, ieder met een bijbehorende eigen geheime sleutel. Zo kunnen bijvoorbeeld een aantal werknemers van een bedrijf ieder afzonderlijk namens hun bedrijf tekenen zonder hun eigen identiteit bekend te hoeven maken. Dergelijke mechanismen kunnen gebruikt worden om aan te tonen dat je bepaalde groepsrechten hebt, op basis van authenticatie als groepslid, en niet als individu. Dat kan privacy en persoonlijke veiligheid ten goede komen.

Er zijn nader onderzoek en nadere experimenten nodig om dergelijke innovatieve technieken praktisch nuttig en commercieel aantrekkelijk te maken. Maar bovenal is er een politieke en maatschappelijke wil voor nodig.

Hoofdstuk 9

Identiteitsfraude en attribuutfraude

Een tijd geleden zaten een middag lang een aantal onbekende hangjongeren op het hek voor ons huis luidruchtig te praten en te roken. Op een gegeven moment was mijn vrouw het zat en stuurde ze weg. Prompt werden er een aantal grote pizza's aan de deur bezorgd. Ze heeft geweigerd die pizza's aan te nemen, ondanks aandringen van de bezorger die als argument gebruikte dat het adres klopte. Het onderliggende issue is dat de pizza service slechts gebruik maakt van identificatie (het adres), maar niet van authenticatie (bewijs van identiteit). Daardoor worden bepaalde bedrijfsrisico's gelopen. Kennelijk zijn die acceptabel want dit model wordt al jaren gehanteerd.

De hangjongeren maakten zich schuldig aan identiteitsfraude: ze deden zich voor als een ander, namelijk als iemand die woonde op ons adres, en plaatsten vanuit die aangenomen identiteit een bestelling. De negatieve gevolgen daarvan zijn meestal voor degene met de ware identiteit. In dit pizza-verhaal lag de last en de financiële schade niet echt bij ons, maar vooral bij de pizzabakker.

Identiteitsfraude is van alle tijden. Ik herinner me van vroeger dat een onpopulaire persoon in de buurt ooit een complete encyclopedie thuisbezorgd kreeg. Rijden met valse kentekenplaten is ook een voorbeeld, of het tonen van een vervalst paspoort. Zelfs in de gevangenissen komt het opvallend vaak voor—tot meer dan 5% wordt wel genoemd[1]—dat iemand anders dan de veroordeelde de straf uitzit. In ons digitale tijdperk is identiteitsfraude echter een veel ernstiger probleem geworden. Bij communicatie via digitale netwerken weet je nu eenmaal in principe niet wie er aan de andere kant van de lijn zit, waardoor de mogelijkheden tot misbruik groter zijn. Ik ken geen Nederlandse cijfers, maar in de Verenigde Staten is identiteitsfraude de snelst stijgende vorm van misdaad. Het gaat dan bijvoorbeeld om online fraude via credit card of *social security* nummers[2]. Breed gebruik van ons BSN nodigt er ook toe uit.

Bij identiteitsfraude slaagt een ander erin zich als jou voor te doen, met alle verve-

[1] Zie: Jan Grijpink, Identiteitsfraude en Overheid. Justiële Verkenningen 7, 2006 (ihb. p. 45), beschikbaar via `www.wodc.nl`.

[2] Zie bijvoorbeeld de Amerikaanse en Engelse websites `www.consumer.gov/idtheft` en `www.identity-theft.org.uk`. Maar ook in Nederland krijgt het onderwerp langzaamaan meer aandacht.

lende consequenties vandien. Identificatie als jou is vaak niet zo moeilijk in situaties waarin alleen een naam of een naam plus adres of geboortedatum of BSN vereist is. Authenticatie is wat identiteitsfraude moet voorkomen, bijvoorbeeld via een handtekening, PIN of paspoort. Niet al die middelen zijn echter geschikt voor gebruik via netwerken. Daarbij worden bij authenticatie meestal gegevens gevraagd die bij jou specifiek horen, zoals een wachtwoord, of een gegeven dat bijna niemand anders weet, zoals de meisjesnaam van je moeder. Authenticatie op basis van zo'n 'geheim' is niet zo sterk, zeker niet op de lange termijn: wanneer u overal de meisjesnaam van uw moeder moet noemen raakt die naam steeds breder bekend waardoor het risico toeneemt dat iemand anders die achternaam een keer misbruikt om zich onterecht als u voor te doen. Hierbij hanteer ik overigens de traditionele aanname dat u de achternaam van uw vader draagt.

Er worden echter steeds meer gegevens die eigen aan ons zijn opgeslagen in centrale databanken. Al die gegevens zouden misbruikt kunnen worden voor identiteitsfraude. Veel van die databanken hangen aan het internet, waardoor ze kwetsbaar zijn voor elektronische inbraken. We kennen allemaal de verhalen van hackers die binnengedrongen zijn in databanken met credit card nummers of inloggegevens. Ook door slordigheid worden zulke databanken soms verkeerd aan het internet gekoppeld waardoor veel te veel gegevens toegankelijk zijn. Misbruik door insiders wordt vaak onderschat, maar komt in de praktijk vaker voor dan misbruik door outsiders.

Het internet heeft identiteitsfraude dus verergerd, niet alleen omdat authenticatie lastiger is, maar ook omdat meer persoonlijke gegevens (bedoeld of onbedoeld) toegankelijk zijn via identiteiten. Daarnaast kan een eenmaal gestolen identiteit vaak voor meerdere doeleinden misbruikt worden, waarbij de dader anoniem en veilig op afstand zit. Door systematisch te googlen kun je veel over iemand te weten komen, en je daarmee makkelijker als die persoon voordoen. Ook door gewiekst, charmant, of aandringend via telefoon of email, mogelijk reeds onder een andere naam, door te vragen kun je vaak veel informatie oneigenlijk bemachtigen. De term die daarvoor in de beveiligingswereld gebruikt wordt is *social engineering*. De bekende (voormalige) hacker Kevin Mitnick beweert meer gevoelige informatie te hebben verkregen via *social engineering* dan via inbraken.

We staan dus bloot aan steeds grotere gevaren met betrekking tot onze identiteit. Wat kunnen we daar zelf aan doen? De eerste regel is en blijft: nooit meer gegevens over jezelf weggeven dan strikt noodzakelijk is. Wat anderen niet weten kunnen ze ook niet misbruiken. Een tweede regel is: achterdochtig zijn. Weet ik wel zeker dat degene die ik aan de lijn heb is wie hij zegt te zijn? En: als je al persoonsgegevens weggeeft, controleer dan eerst goed of je wel met de juiste partij te maken hebt, bijvoorbeeld via het eerdergenoemde slotje in je webbrowser. Op de langere termijn kunnen we ook ijveren voor het invoeren van een veiliger, meer gedecentraliseerd beheer van identiteiten, in de politiek, via de pers en publieke opinie en ook in het bedrijfsleven: *vote with your dollars*, zoals de Amerikanen zeggen; niet kopen en niet gebruiken wat je niet vertrouwt.

En wat kunnen de organisaties doen die dit soort systemen voor het beheer van

identiteiten (voor *identity management*, in het engels) inrichten en beheren? Hier zie je twee tegengestelde strategieën: identiteiten meer of juist minder gebruiken.

De eerste lijn is gericht op intensiever en meer gecontroleerd gebruik van identiteiten: sterkere authenticatie, meer monitoring en controle, en vaak ook meer centralisatie. De achterliggende idee is om frontaal de strijd aan te gaan en de fraude echt te bestrijden. Dit is een natuurlijke reflex ("we pakken alle boeven op!"), maar het is een historisch gegeven dat zoiets nooit volledig lukt. Ook is het zo dat wanneer je meer (economische of veiligheids-) waarde gaat hechten aan authenticatie, identiteitsfraude zich juist meer gaat lonen: wanneer mensen veel vertrouwen hebben in identiteitsdocumenten is er met een gefraudeerd document dus ook meer te bereiken.

De tweede lijn is meer gericht op preventie, en op het 'identiteitsarm' maken van processen. Wanneer identiteiten beperkt gebruikt worden, loont fraude ook minder. Bij deze strategie worden de risico's voor individuen centraal gesteld. Voor veel organisaties is dit op een of andere manier niet de meest voor de handliggende weg, waarschijnlijk omdat het ze minder additionele controle en macht geeft over de betrokken individuen (burgers, klanten). Toch is het deze aanpak met gefragmenteerde deel-identiteiten die toegesneden zijn op een bepaalde rol of taak die het beste lijkt aan te sluiten op de manier waarop mensen in het dagelijkse leven met elkaar omgaan, en die de basis vormt voor onze op individuele autonomie en verantwoordelijkheid gebaseerde samenleving.

Identiteitsfraude overstijgt het persoonlijke belang. Voorheen was het zo dat het vooral je eigen verantwoordelijkheid was om zorgvuldig met je persoonsgegevens om te gaan. Als jij er zelf slordig mee omgaat en daardoor zelf benadeeld of in verlegenheid gebracht wordt ben je zelf een sukkel en heb je vooral zelf een probleem. Identiteitsfraude is echter een groot maatschappelijk probleem aan het worden, niet alleen door de sterk gegroeide omvang maar ook door de ernst van de misdaden (criminaliteit, terrorisme) die ermee samenhangen. Daarmee heeft de overheid er alle belang bij dat mensen over adekwate middelen en rechten (en het bijbehorende besef) beschikken om hun persoonsgegevens te beschermen. Onderdeel daarvan is dat mensen zelf effectief kunnen vaststellen met wie of wat ze te maken hebben voordat ze gegevens overdragen: bij gevoelige transacties hoort de omgeving zich dan ook eerst te authenticeren. Deze 'gouden regel' zagen we al eerder, in Hoofdstuk 4.

Attribuutfraude

Als individu wordt je dagelijks geconfronteerd met formulieren waarin om persoonlijke informatie gevraagd wordt, meestal om een of andere dienst of product te verkrijgen. Daarbij is het vaak niet eenvoudig om zelf uit te maken welke informatie strikt noodzakelijk is voor de gewenste dienst. Bij het aanvragen van een kortingskaart voor de Nederlandse Spoorwegen (NS) wordt bijvoorbeeld de geboortedatum en het geslacht gevraagd. Waarom eigenlijk? Vaak wordt er ook geen onderscheid gemaakt tussen informatie die noodzakelijk is voor de gevraagde dienst en informatie die slechts gebruikt wordt om een profiel van de klant op te kunnen stellen (en daarmee

voor marketing doeleinden). Zodra ik het gevoel krijg dat het om profileringsvragen gaat vul ik onsamenhangende onzin in[3].

De enige effectieve mogelijkheid van verdediging tegen dit soort praktijken is wat ik ‘attribuutfraude’ wil noemen: het bewust verstrekken van gedeeltelijk onjuiste gegevens, maar op zodanige wijze dat de gewenste dienst wel toegekend wordt. Op de universiteit heb ik bij een college eens aan de aanwezige studenten (een zestigtal) gevraagd wie er een hotmail account had: bijna iedereen. En ook wie er bij het aanvragen daarvan alle gevraagde informatie correct had opgegeven: bijna niemand!

Grote databanken met klantgegevens zitten dus vol met fouten, zeker wanneer klanten zelf een deel van de gegevens kunnen opgeven. Hierdoor wordt de bruikbaarheid van zulke databanken ernstig aangetast: de conclusies die erop gebaseerd worden zijn dus niet volledig betrouwbaar. Het centralistische model heeft zijn beperkingen, simpelweg omdat de menselijke maat ontbreekt en de individuen om wie het gaat er vaak geen vertrouwen in hebben. Centralisatie leidt tot vervreemding. In een meer gedecentraliseerde opzet waarbij mensen hun eigen gegevens makkelijk kunnen beheren en controleren is individuele betrokkenheid—met bijbehorende bereidheid tot het gebruiken van juiste gegevens—een stuk groter en is de mate van vervreemding tegenover ‘het systeem’ navenant geringer. Wanneer individuen door organisaties—of door zichzelf, in toenemende zelfgerichtheid—werkelijk serieus genomen worden vormt personalisatie via decentraal gegevensbeheer de natuurlijke weg.

[3]Mijn favoriete geboortedatum is iets als 29 feb. 1950, maar helaas zijn de meeste hedendaagse systemen zo slim om na te gaan dat dit geen bestaande datum is. Ik probeer het toch vaak. Bij de NS verwacht ik binnenkort een aanbieding voor een seniorenkaart. Dit is bij mij een melige sport geworden.

Hoofdstuk 10

Bonnetjes, zegeltjes en bonuspunten

Stel ik ga naar de bioscoop of naar het theater en geef bij de garderobe mijn jas af. Meestal werkt het dan zo dat ik een eenvoudig genummerd bonnetje krijg waarmee ik aan het einde van de avond mijn jas weer terug kan krijgen. Dit systeem is anoniem, want aan de garderobe weet men niet wie ik ben. Misschien onthoudt de garderobedame wel iets persoonlijks van mij—die man met die versleten jas en charmante glimlach—maar daar krijg ik mijn eigendom waarschijnlijk niet mee terug. Voor de werking van het systeem is het ook helemaal niet nodig dat ik mij met naam en toenaam identificeer. Het genummerde bonnetje is in principe genoeg. Het bepaalt mijn ‘tijdelijke garderobe-identiteit’.

Dit bonnetjessysteem is natuurlijk niet erg veilig. Meestal wordt er een boekje met standaard gekleurde bonnetjes gebruikt van het soort dat overal verkrijgbaar is. Ik zou bijvoorbeeld zelf zo’n boekje kunnen kopen, en dan aan het eind van een bijzondere balletvoorstelling snel met een paar eigen bonnetjes naar de garderobe kunnen rennen in de hoop er met een paar dure bontjassen vandoor te kunnen gaan, voordat de rechtmatige eigenaren verschijnen. Het onderliggende probleem is dat de echtheid (ofwel integriteit en authenticiteit) van de bonnetjes niet of nauwelijks gegarandeerd is. Toch werkt het systeem in de praktijk redelijk. Er is kennelijk voldoende onderling vertrouwen om een dergelijk relatief zwak systeem naar behoren te laten functioneren. Heeft u ooit over zulke risico’s nagedacht bij het afgeven van uw jas?

Natuurlijk zijn er veiliger versies te bedenken. Men zou speciaal gedrukte bonnetjes kunnen gebruiken die niet overal verkrijgbaar zijn en ook moeilijker nagemaakt kunnen worden. Ook zou men bonnetjes met grotere getallen (in willekeurige volgorde) kunnen gebruiken, bijvoorbeeld met vijf cijfers. De kans dat het nummer op mijn nepbonnetje ook daadwerkelijk gebruikt wordt op de avond waarop ik toesla is dan een stuk kleiner. Ook kan gevraagd worden of de brenger van een jas een handtekening zet op het bonnetje dat op de jas achterblijft in de garderobe. Bij het ophalen dient dan ook een handtekening gezet te worden ter controle. Men kan het ook in de techniek zoeken en bijvoorbeeld bij het afgeven van de jas een vinger op een vingerafdruklezer laten leggen. Een computer kan dan aan de vingerafdruk een plaats op de kapstok koppelen, waar de jas door het garderobepersoneel opgehangen wordt. Er zijn dan

geen bonnetjes nodig, waardoor het risico van het kwijtraken van het bonnetje vervalt. Bij het ophalen hoeft slechts de vinger opnieuw op de lezer geplaatst te worden, zodat de computer na herkenning de bijbehorende plek aan het personeel kan tonen. Sommige mensen zouden zoiets prachtig vinden, terwijl anderen gruwen bij een dergelijk gebruik van biometrie (alweer mijn vingerafdruk afgeven; wat gebeurt ermee?). En natuurlijk introduceren zulke technieken weer nieuwe risico's, bijvoorbeeld op chaos bij uitval. Hoe dan ook, we hebben het hier over oplossingen voor een niet bestaand probleem. Een tijdelijke deel-identiteit is voldoende voor een systeem waar iedereen al jaren mee bekend is en naar tevredenheid gebruik van maakt.

Voor veel situaties zijn zwakke identiteiten inderdaad voldoende. Wanneer ik een nieuw strijkijzer koop wil ik graag een garantiebewijs. Daarvoor hoeft de winkelier mij niet persoonlijk te kennen. Het is voldoende dat hij mij een volgende keer herkent als iemand die eerder (binnen de garantietermijn) een strijkijzer gekocht heeft. Meestal wordt zoiets geregeld via een fysiek garantiebewijs met een datumstempel. Wanneer de winkelier toch vraagt om bijvoorbeeld naam en adres op te geven heeft dat in principe niets te maken met garantie, maar alles met marketing: men wil de klant kennen om een profiel op te bouwen zodat reclame beter gericht kan worden.

Nu kunt u zich er misschien niet zo heel erg druk over maken of u nu wel of niet als strijkijzerkoper te boek komt te staan. Maar misschien maakt dat wel wat uit als het gaat om prozac, viagra of aambeienzalf.

Wanneer mijn aankoop via het web plaatsvindt zou een garantiebewijs kunnen bestaan uit een garantieverklaring met een datum, waaronder de webwinkelier een digitale handtekening gezet heeft. Ook daarvoor is mijn identiteit niet nodig. Natuurlijk heeft de leverancier wel mijn adres nodig. In sommige gevallen is een garantiebewijs persoonsgebonden en niet overdraagbaar. In dat geval zou het bewijs aan een tijdelijke identiteit van mij gebonden kunnen worden, net als een garderobebonnetje met handtekening. Ik moet die tijdelijke identiteit natuurlijk wel bewaren, voor eventueel later gebruik wanneer ik de garantie nodig heb.

Zegeltjes

Nederlanders krijgen soms het verwijt een kruideniersmentaliteit te hebben. Zeker is dat kruideniers in Nederland de mentaliteit van hun klanten goed kennen, en weten dat ze nergens zo enthousiast voor te krijgen zijn als voor zegeltjesacties. Voor onbenullige voordeeltjes verspillen mensen hun eigen kostbare tijd en moeite om boekjes vol te plakken en laten ze zich gedwee binden aan een bepaalde grutter.

Toch is het de moeite waard om zegeltjes vanuit identiteitsperspectief nader te beschouwen. Zegeltjes zijn anoniem, en daarmee makkelijk overdraagbaar, zoals bekend uit schaamteloze verzoeken aan de kassa: "Oh, mag ik dan uw zegeltjes?". Ook beschrijven zegeltjes het gedrag van de klant maar in beperkte mate: ze worden typisch toegekend op basis van de hoogte van het aankoopbedrag, en niet op basis van de aard van de aankoop. Wel vertegenwoordigen zegeltjes een bepaalde waarde, zij het minimaal. Die waarde is in feite zo gering dat waarschijnlijk niemand het in zijn hoofd zal

halen om nepzegeltjes te gaan maken. Zegeltjes zijn dus wel waardepapieren waarvan de echtheid in principe van belang is. Ook interessant is dat zegeltjes aan de klanten zelf in beheer gegeven worden. Er is sprake van een gedecentraliseerd systeem. De kruidenier zou ook tegen de klant kunnen zeggen: ik beheer uw zegels wel centraal, en laat wel weten wanneer uw kaart vol is. Maar zo'n kruidenier is natuurlijk wijzer, en laat het domme plakwerk aan anderen over. Het dumpen van werk (en risico's) op klanten is een beproefde commerciële strategie, die bijvoorbeeld ook aan de basis ligt van internetbankieren of elektronische aangifte.

Bonuspunten

Via zegeltjes probeert de winkelier de klant te binden, maar leert de winkelier de klant niet kennen. Waarom zou een winkelier mij als klant eigenlijk willen kennen? De basis van onze commerciële omgang is dat zij levert en ik betaal. Zolang ik dat doe heeft een winkelier toch verder niks met mij te maken? Westerse tolerantie is voor een groot deel hierop gebaseerd.

Maar een winkelier wil wel dat ik terugkom en dan weer wat koop. Zij wil mij naar de winkel lokken en zodra ik binnen ben zodanig benaderen dat ik enthousiast mijn geld uitgeef. Allerlei 'direct marketing' technieken worden toegepast om ervoor te zorgen dat ik bij de kassa mijn portemonnaie helemaal omkeer. Wat lijkt te werken is het persoonlijk benaderen van klanten, bijvoorbeeld met popie begroetingen als: "Hoi Bart, leuk je weer te zien; wij hebben vandaag speciaal voor jou iets in de aanbieding. Gezien je eerdere aankopen heb je daar vast en zeker behoefte aan." Bij zo'n welkomstboodschap sta ik zelf direct weer buiten, maar in het algemeen schijnt het te werken. De online boekwinkel Amazon maakt ook uitgebreid gebruik van zulke technieken.

Waar het hierbij op neerkomt is om profielen van klanten op te stellen, zodat ze gerichter en persoonlijker benaderd kunnen worden: wanneer blijkt dat u de pil niet meer koopt wordt u bestookt met advertenties voor luiers. Soms gaat dat mis, bijvoorbeeld bij aanvang van de overgang, maar commerciële profielen hoeven ook niet honderd procent te kloppen. De klanten worden in een aantal categorieën ingedeeld, zoals bijvoorbeeld wel of niet met kinderen, vleesetend, koopjesjager, enzovoort.

Maar hoe herkent een winkelier u eigenlijk? Daarvoor laat zij u geheel vrijwillig rondlopen met een identiteitskaart, de zogenaamde bonuskaart. De motivatie om zo'n kaart mee te nemen en bij iedere aankoop te tonen is een financiële: ofwel u krijgt enige korting bij de kassa, en dan vaak alleen op zaken waar de winkelier sowieso van wil, ofwel u kunt bonuspunten sparen voor korting elders, bijvoorbeeld bij een attractiepark. Bij het scannen van de bonuskaart aan de kassa worden de aankopen centraal opgeslagen onder het nummer van uw bonuskaart. Op basis van die geschiedenis van aankopen wordt er een profiel van u opgesteld.

Een win-win situatie: de winkelier kan gerichter adverteren—ongericht adverteren is duurder en minder effectief—en kan het assortiment gerichter kwijtraken; de klant wordt persoonlijk en service-gericht benaderd—en krijgt ook nog eens korting. Dat

laatste is trouwens twijfelachtig, want de winkeliers zouden ook zonder bonuskaarten kunnen werken en alle prijzen iets verlagen. Maar daar gaat het nu niet om.

Maar ondertussen zijn er wel enorme centrale databanken met klantprofielen. Het gaat daarbij om privacygevoelige gegevens, waardoor winkeliers volgens de Wet Bescherming Persoonsgegevens aan strenge eisen moeten voldoen met betrekking tot beheer en beveiliging. Dat brengt extra kosten en risico's met zich mee. Onder de klanten bestaat ook een zekere ongemakkelijkheid over deze grootschalige opslag en profilering. Niet iedereen is ervan gecharmeerd dat alle aankopen (inclusief bijvoorbeeld gevoelige medische zaken) geregistreerd en bewaard worden, en mogelijk ooit ergens naar boven komen en tot een ongemakkelijke confrontatie kunnen leiden. Verder zijn er mensen (zoals schrijver dezes) die wel de bonuskorting willen, maar niet de registratie van gegevens, en daarom zoveel mogelijk saboteren, bijvoorbeeld door regelmatig met anderen van bonuskaart te wisselen. De betrouwbaarheid (en dus ook de bruikbaarheid) van de gegevens in de databanken is dus twijfelachtig.

Zegeltjesprofielen

Op basis van het voorafgaande zou je mogelijk het beste van zegeltjes en bonuspunten willen combineren: laat de klant zelf het eigen profiel bijhouden, alsof het om zegeltjes ging. Laat de klant zelf gepersonaliseerde zegeltjes plakken die recht geven op korting wanneer de winkelier het zegeltjesboekje in de winkel in mag zien—en op basis daarvan persoonsgerichte aanbiedingen kan doen. Hiermee kunnen winkeliers pas echt moeite en risico's dumpen.

Zo'n decentrale benadering lijkt veel voordelen te hebben, maar vereist wel meer infrastructuur. Klanten moeten een uitgebreidere klantenkaart (met geheugen) hebben, of ruimte ter beschikking stellen op GSM of handcomputer om de eigen profielen op te slaan. Technisch hoeft het geen probleem te zijn. De integriteit en authenticiteit van de bij de klant opgeslagen profielen kan met een digitale handtekening van de winkelier gegarandeerd worden. Klanten zullen zich meer op hun gemak voelen omdat ze meer controle hebben over hun eigen gegevens. Dit beheer vereist een intuitieve interface, met begrijpelijke standaardinstellingen. Je kunt je er allerlei extra mogelijkheden bij voorstellen, bijvoorbeeld hoe verder het profiel teruggaat in de geschiedenis, hoe groter de korting. Dat motiveert mensen om lang mee te doen. Je zou mensen ook de mogelijkheid kunnen bieden om bepaalde aankopen uit hun eigen profiel te verwijderen—bijvoorbeeld de combinatie van *Playboy* en doos tissues. Dat is pas persoonsgerichte service, uitgaande van vertrouwen in en respect voor de klant.

Een dergelijke benadering verschilt hemelsbreed van wat ik 'Stasi' automatisering zou willen noemen: schiet iedere klant een chip in de nek, volg alle bewegingen en handelingen door de hele winkel en sla die tezamen met de aankopen op in de centrale databank. Waar kiezen we voor?

Hoofdstuk 11

Identiteiten en attributen

We hebben in het vorige hoofdstuk gezien dat identiteiten lang niet altijd nodig zijn om een transactie uit te kunnen voeren. Vaak is het genoeg om een aantal eigenschappen (attributen) van betrokkenen te kennen. Volgens de Nederlandse wet mag bijvoorbeeld geen alcoholhoudende drank verkocht worden aan jongeren onder de 16 jaar en geen sterke drank aan jongeren onder de 18. Wie dat toch verkoopt is strafbaar. Winkeliers kunnen daarom om een persoonsbewijs, zoals identiteitskaart, paspoort of rijbewijs vragen. Zo'n bewijs geeft echter veel te veel informatie. Wanneer je het nieuwe biometrische paspoort aan een winkelier geeft kan hij het volledig uitlezen, en daarmee niet alleen je geboortedatum, maar ook je naam, BSN etcetera in zijn computer opnemen, compleet met digitale foto. Dat is natuurlijk handig voor een goed elektronisch klantenbestand, maar buiten proportie voor de (wettigheid van de) transactie waar het eigenlijk om gaat. Daar is slechts 'leeftijds' authenticatie voor nodig, via een soort onderhandelingsproces waarbij de betrokkene controle houdt over wat er allemaal overgedragen wordt.

Wat je in zo'n situatie, zeker in de online wereld, zou willen hebben is een geautoriseerde minimale verklaring van de vorm "de persoon die voor u staat is ouder dan 18". Wie die persoon verder is doet er niet toe. Zo'n verklaring zou digitaal ondertekend kunnen worden door de gemeente, en toegezonden op het moment dat een ingezetene de 18-jarige leeftijd bereikt. Zo'n verklaring heet een attribuutcertificaat, of ook wel *credential*. Een attribuutcertificaat is anders dan een identiteitscertificaat (zoals besproken in Hoofdstuk 8) omdat er geen koppeling wordt gelegd tussen een identiteit en een publieke sleutel, maar tussen een of meerdere eigenschappen (attributen) en zo'n sleutel.

Een ander voorbeeld. De vuilnisstort in mijn gemeente is alleen toegankelijk voor de eigen inwoners. Iedereen begrijpt dat. Wanneer ik afval wegbreng wapper ik even met mijn rijbewijs. Er wordt dan vluchtig gecontroleerd, maar niets bijgehouden. Echter, 'digitaal wapperen' bestaat niet. Wanneer je niet alle gegevens van je digitale identiteitsdocument af wil geven heb je een attribuutcertificaat nodig, zoals bijvoorbeeld 'inwoner van Nijmegen'. Dat is precies genoeg voor de vuilnisstort, maar mogelijk ook voor bepaalde andere diensten op de webstek van de gemeente. Je kunt je

voorstellen dat gemeenten hun inwoners een setje digitale attribuutcertificaten geven, bijvoorbeeld wanneer ze de achtienjarige leeftijd bereiken. Daarmee kunnen de inwoners adequaat van allerlei diensten gebruik maken, zonder dat ze direct het risico lopen bloot gesteld te worden aan identiteitsfraude: wanneer ik alleen een paar relevante attributen toon zonder mijn identiteit prijs te geven kan een kwaadwillende zich daarmee ook niet als mij voordoen.

Het onderliggende issue is dat autorisatie goed geregeld kan worden zonder identificatie. Uit de voorbeelden blijkt dat autorisaties gegeven kunnen worden op basis van attributen of rollen. De kapitein van een schip is bijvoorbeeld gemachtigd een aantal handelingen te verrichten (of te bevelen), los van wie toevallig die kapitein is. Natuurlijk moet die "toevallige" persoon die beweert kapitein te zijn dat wel kunnen bewijzen. Er is inmiddels een eigen naam, namelijk *role-based access control*, voor deze ziens- en werk-wijze.

Er is hierbij nog wel een subtiel technisch punt dat enige aandacht verdient: wanneer ik overal hetzelfde attribuutcertificaat laat zien kan ik toch via de bijbehorende publieke sleutel getraceerd worden. Er kan echter met technische middelen voor gezorgd worden dat die attribuutcertificaten er iedere keer iets anders uitzien, ook al tonen ze hetzelfde attribuut. Ook kan met zogenaamde blindering en *zero knowledge* technieken gewerkt worden, waarbij geen identificerende informatie met het attribuut weggegeven wordt.

Nu identiteitsfraude steeds ontwrichtender vormen aan begint te nemen en grote op identiteiten gebaseerde databanken steeds meer Orwelliaanse scenario's mogelijk maken is de tijd misschien rijp om op attribuutcertificaten gebaseerde interactie en dienstverlening serieus te nemen en te realiseren.

Hoofdstuk 12

Gegevens en policies

In de digitale wereld waarin we leven produceren wij als individuen steeds meer digitale sporen: betalingen, telefoontjes, reizen, bellen, mailen, surfen enzovoort. Steeds meer van onze gedragingen laten een stroom aan gegevens na. Veel handelingen en diensten die vroeger anoniem plaatsvonden zijn nu zodanig gereorganiseerd dat ze zonder identiteit van de klant niet meer mogelijk zijn, ook wanneer dat strikt genomen helemaal niet nodig is. Kontant betalen wordt steeds meer vervangen door betalen met pinpas of credit card. Treinkaartjes worden vervangen door een OV-chipkaart. Nieuwere vormen van TV vormen een soortgelijke voorbeelden (zie hieronder). Typisch worden dergelijke digitale sporen opgeslagen in grote centrale databanken.

Traditioneel worden door TV-masten alle kanalen uitgezonden, waarvan jij als kijker er dan één met een antenne uit de lucht oppikt. Aan de versturende kant hebben ze er in dit *broadcast* model geen idee van waar jij naar zit te kijken. Meer recente abbonnementen voor digitale televisie zijn typisch gebaseerd op een heel ander model, dat *client-server* genoemd wordt. Jij vraagt als kijker (*client*) aan de aanbieder (*server*) om een bepaald programma te bekijken. Dat programma wordt vervolgens aan jou gericht verstuurd. Plotseling weet de versturende kant precies waarnaar jij zit te kijken. Een mogelijk gevolg is dat wanneer jij bijvoorbeeld twee pornofilms gekeken hebt er een paar dagen later een uitnoding in je brievenbus valt voor een locaal SM-festival. Is dat erg? Je kunt het zien als een vorm van service verlening. Maar het geeft veel mensen denk ik toch een ongemakkelijk gevoel. Nog meer sensors op je lijf! En nog meer persoonlijke risico's wanneer gegevens uitlekken (bewust of door nalatigheid) of gebruikt worden voor chantage. Ik kan me voorstellen dat het toch enige rimpelingen—of op z'n minst ongemakkelijkheid—veroorzaakt wanneer blijkt dat de plaatselijke dominee of kleuterjuf 's avonds laat ooit wel eens naar een opwindende film kijkt—misschien wel met homo-erotische scenes! Er zijn vast ook periodieken die er heel wat voor over hebben (aan geld of moeite) om het kijkgedrag van de koningin in handen te krijgen. Ook dat zal ergens beschikbaar zijn. Moet de koningin—of een willekeurig andere publieke figuur—dan maar geen digitale TV nemen? Of moet zij maar zo goed leren oppassen dat zij met haar kijkgedrag nooit gecompromitteerd kan worden? Of moeten we iets beter gaan nadenken over hoe we dit soort zaken willen structureren?

Waarschijnlijk kan de koningin wel via een of ander pseudoniem een abonnement op digitale TV nemen. Maar waarom zouden u en ik dat dan niet ook kunnen?

Willen wij dit gedrag eigenlijk allemaal wel vastleggen? Zo ja, wie heeft er dan controle over? We lopen daarbij altijd ook nog het risico dat een of andere politicus ferm en stoer over wil komen en gaat verkondigen dat het voor terrorismebestrijding absoluut noodzakelijk is dat er een centrale databank komt van TV-kijkgedrag of van OV-verplaatsingen, waar de overheid naar believen in moet kunnen rondsnuffelen.

Websurfen is altijd al gebaseerd geweest op het *client-server* model. Jouw browser vraagt een webpagina op, die door de server naar jouw computer teruggestuurd wordt. Jouw computer is op het internet door de server terug te vinden via een zogenaamde IP-adres. De meeste mensen (of gezinnen) hebben tegenwoordig een vast IP-adres, zodat via dit adres al het surfgedrag vastgelegd kan worden. Dit kan op twee plaatsen. Je internet provider ziet al je internetverkeer (inclusief email, chat, etc.) voorbijkomen, en weet daarmee in principe alles wat je doet. Maar ook alle verschillende servers op het internet die webpagina's aanbieden kunnen de IP-adressen opslaan van iedereen die een webpagina opvraagt. Op zo'n manier kunnen bijvoorbeeld webradio's bestanden aanleggen van wie wanneer waar naar luistert. Ook zijn er organisaties zoals *doubleclick* die tot doel hebben om individueel surfgedrag via *cookies* in kaart te brengen om de resulterende profielen te verkopen. Sporen op het web worden echter niet alleen voor commerciële doeleinden vastgelegd, maar ook om veiligheidredenen. Er is al Europese regelgeving om internetverkeersgegevens van alle 500 miljoen Europeanen voor langere tijd vast te leggen, inderdaad, omwille van de terrorismebestrijding.

Een centrale vraag is: van wie zijn eigenlijk de digitale sporen die jij nalaat? Hier is geen eenvoudig antwoord op te geven, maar ik meen dat veel mensen gevoelsmatig toch het idee hebben dat zulke gegevens vooral henzelf toebehoren en niet zozeer iemand anders.

Opslag van zulke digitale sporen is vaak vereist om bepaalde diensten te kunnen bieden of om af te kunnen rekenen. Maar vaak ook wordt er veel meer dan functioneel noodzakelijk is opgeslagen omwille van profilering. Het is altijd zinvol kritisch na te gaan of die opslag gekoppeld moet zijn aan expliciete identiteiten, of dat ook een identiteitsarme benadering mogelijk is, bijvoorbeeld op basis van pseudoniemen of attributen. We komen dan op het gebied van de zogenaamde *Privacy Enhancing Technologies* (PETs). Maar misschien is een meer radicale omschakeling wel mogelijk, waarbij de relevante gegevens juist niet centraal, maar decentraal en onder directe controle van betrokken individuen, opgeslagen wordt.

Medische gegevens

Ook in de medische wereld neemt digitalisering toe. Deze ontwikkeling leidt bijvoorbeeld tot snellere en preciezere diagnoses en tot betere controle bij de behandeling. Ook behoort monitoring en behandeling op afstand steeds meer tot de mogelijkheden, waardoor ouderen bijvoorbeeld langer en comfortabeler thuis kunnen blijven wonen. Er wordt op dit moment al geëxperimenteerd met woonomgevingen vol medische sensors, waardoor continue bewaking mogelijk is. Dit leidt tot een grote stroom privacygevoelige medische gegevens over je geestelijke en lichamelijke toestand en gedragingen, tot en met de frequentie, omvang en samenhangendheid van je ontlasting. Dat is dan niet meer iets wat je vertrouwelijk met je huisarts bespreekt, maar iets wat in digitale vorm door netwerken flitst en rechtstreeks in je persoonlijke dossier in een grote databank komt.

Van wie zijn al die medische gegevens over jou eigenlijk, en wie zou er het beste de controle over kunnen hebben? Ook dit zijn fundamentele vragen, waar niet zo snel een eenduidig antwoord op te geven is. De Nederlandse wet kent bewust geen eigendom toe, noch aan de verantwoordelijke medicus, noch aan de patiënt.

In veel westerse landen wordt de laatste jaren gewerkt aan elektronische patiëntendossiers (EPDs). De bedoeling is om de efficiëntie te vergroten, zowel van het behandelproces als van de behandeling. Dat laatste kan doordat een arts via zo'n dossier beter met collega's communiceert en daardoor een beter (historisch) overzicht heeft, waardoor er (hopelijk) minder fouten gemaakt worden, bijvoorbeeld met betrekking tot medicijnen die niet gecombineerd kunnen worden. Ook zou speciaal toegesneden software de dossiers periodiek kunnen controleren op zulke inconsistenties.

De invoering van zo'n EPD is een gigantische organisatorische operatie, mede omdat de medische zorgverlening gefragmenteerd is in vaak kleine autonome eilandjes die ieder hun eigen automatiseringsbeleid voeren. Ook vergt zo'n EPD een redelijke mate van overeenstemming over de formaten waarin de gegevens verwerkt worden. Deze issues zijn echter niet waar het me hier om te doen is.

Hoe zouden zulke EPDs georganiseerd en beheerd moeten worden? Een eerste naïeve gedachte is om alle EPDs in een centrale databank op te slaan. Dit is niet verstandig, niet alleen omdat deze databank een onvoorstelbare hoeveelheid gegevens moet kunnen bevatten en erg veel transacties moet kunnen afhandelen, maar ook omdat er een onaanvaardbaar bedrijfsrisico ontstaat: deze databank vormt een *single point of failure*. Wanneer deze databank plat gaat kan er niemand in Nederland meer medisch behandeld worden. Daarnaast vormt deze ene databank een groot privacy risico. Er zou moedwillig geprobeerd kunnen worden om de medische gegevens van bijvoorbeeld bekende Nederlanders uit te lezen, of zelfs te veranderen. En aan de consequenties van eventueel 'omvallen' van zo'n databank waarbij de inhoud op straat komt te liggen wil je al helemaal niet denken.

Een tweede gedachte is om geen centrale databank, maar wel een centrale verwijzingsindex op te zetten. Dit is in feite waar in Nederland voor gekozen is, onder de naam Landelijk Schakel Punt. De medische gegevens van mij blijven gefragmenteerd bestaan bij de verschillende behandelaars die ik bezocht heb, maar de centrale index bevat verwijzingen naar al die losse brokjes die tezamen mijn EPD vormen. Via dit schakelpunt zijn alle losse onderdelen van mijn dossier snel te vinden, waarbij de kwetsbaarheid van centrale opslag vermeden wordt.

Toch is er nog een derde mogelijkheid: geef het EPD aan de betreffende persoon zelf. Het zijn tenslotte gegevens van die persoon zelf. In eerste instantie roept dit misschien bevreemding op, maar de onderliggende gedachte is zeer redelijk: het EPD

bevat zeer gevoelige en persoonlijke informatie die makkelijk misbruikt kan worden en daarom maar het beste aan mensen zelf in eigen beheer gegeven kan worden. Wanneer ik dan een arts bezoek geef ik de arts op dat moment (of enige tijd tevoren) tijdelijk toegang tot mijn dossier. De arts voegt gedurende de behandeling nieuwe gegevens toe aan het dossier, uiteraard voorzien van de juiste digitale handtekening om integriteit en authenticiteit te garanderen.

Sinds enige jaren gebruik ik een handcomputer (ofwel *Personal Digital Assistant*, of PDA). In de adreslijst bij mijn huisarts houd ik een apart bestandje bij met daarin mijn eigen informele medische dossier. Na ieder bezoek noteer ik de datum, mijn klacht, en het advies van de huisarts. Bij een volgend bezoek kan ik dan snel nazien wat (en wanneer) eerder besproken is. Dit mini-dossier heeft natuurlijk geen enkele officiële status. Ik vind het wel aangenaam en handig om zelf een beter overzicht te hebben.

Is nu de suggestie dat het gehele medische dossier maar verplaatst moet worden naar de eigen handcomputer (PDA), laptop of PC? Ja en nee. Wat waarschijnlijk niet gewenst is dat individuele medische dossiers bij mensen thuis enkel op hun eigen PCs staan die meestal voorzien zijn van onbetrouwbare computerprogramma's en besmet zijn met allerlei soorten kwaadaardige software zoals virussen en wormen. Maar we zouden wel nader kunnen nadenken over een soort persoonlijke digitale kluis waartoe de toegang geregeld is via cryptografische sleutels die bij individuen zelf in beheer gegeven worden. Iedereen is dan vrij om delen van het eigen EPD te downloaden naar de eigen PC of PDA. Een uittreksel met essentiële gegevens op je PDA kan inderdaad handig zijn. Dan hoef ik het zelf niet meer allemaal bij te houden in mijn eigen medische schaduwboekhouding.

Het idee van zo'n digitale kluis is eerder gesuggereerd[1] maar is nog nooit systematisch uitgewerkt. Je wil er waarschijnlijk wel een digitale noodknop aan toe voegen zodat een medische hulpverlener in noodsituaties, bijvoorbeeld wanneer je bewusteloos ligt na een ongeluk, toegang heeft tot jouw EPD. Zo'n noodknop vereist dan wel authenticatie als hulpverlener, met een verantwoording achteraf.

De precieze locatie van zo'n digitale kluis in een gridnetwerk van computers is feitelijk niet zo belangrijk zolang de toegang maar gereguleerd is via cryptografische sleutels van de eigenaar. Wel belangrijk is de vereiste verandering van paradigma: differentiatie en decentralisatie in plaats van uniformiteit en centralisatie, waarbij macht en controle in handen van individuen ligt, en niet in handen van steeds abstractere en onpersoonlijkere partijen. Ook hier is decentralisatie essentieel voor een menselijke maat.

Policies

Stel we hebben een zodanige staat van verlichtheid in onze samenleving bereikt dat individuen inderdaad zelf het beheer hebben over hun EPD. En stel dat ik in zo'n situatie

[1] In 2001 door een adviescommissie voor de modernisering van de GBA onder leiding van Snellen.

een verpleger (maar geen arts) bezoek voor een routine controle van mijn bloed. Ik zou die verpleger (na authenticatie, natuurlijk) toegang kunnen geven tot mijn medische dossier onder de volgende condities: u mag enkel vandaag alleen mijn bloedgegevens zien, u mag er wat aan toevoegen indien u er uw digitale handtekening onder zet, maar u mag er niets aan veranderen (want dat is voorbehouden aan artsen). Zulke condities vormen een voorbeeld van een *policy*.

De hier beschreven *policy* is erg strikt, omdat ik een achterdochtig pietje precies ben. Anderen zijn misschien wat soepeler (of luier) en geven de genoemde bloedprikker direct toegang tot het hele eigen dossier. Misschien is dat wel hun zelfgekozen standaardpolicy. Weer anderen schamen zich misschien voor bepaalde onderdelen van hun medische dossier en hanteren daarom ook zeer restrictieve policies. Hoe dan ook, zo'n *policy* geeft een eigen persoonlijke keuze weer over hoe anderen met de persoonlijke gegevens om moeten gaan.

In het algemeen beschrijven *policies* gebruiksbeslissingen: regels die het gebruik van gegevens door anderen zouden moeten bepalen. Soms gaat het dan over persoonlijke gegevens, maar vaak ook helemaal niet. Digitale muziek die op het internet (legaal) aangeboden wordt is vaak voorzien van een bepaalde *policy*. Bij Apple's iTunes is bijvoorbeeld toegestaan om gekochte digitale muziek op maximaal vijf verschillende computers af te spelen, en op een ongelimiteerd aantal iPods. Ook in het privacy onderzoek wordt nagedacht over *sticky policies*, die aan gegevens gehecht worden en het gebruik ervan moeten reguleren.

Het mechanisme voor de handhaving van zulke policies (voor muziek of films) heet *Digital Rights Management* (DRM). Het woord 'rights' is opportunistisch, net als 'service' in Burger Service Nummer (BSN). De 'R' kan beter voor '*restrictions*' gebruikt worden (en de 'S' voor 'spionage'). Zulke DRM mechanismen zijn zeer omstreden omdat ze kopers aan gebruiksbeperkingen onderwerpen en vaak oneigenlijk ingezet worden om de concurrentie dwars te zitten. DRM technieken zijn daarom een populair doelwit onder hackers die er steeds in slagen ze te doorbreken. Denk maar aan DVDs waarvan het beschermingsmechanisme CSS snel omzeild was.

Er is hier echter sprake van een overeenkomstig belang tussen platenbazen die het gebruik van hun muziek onder controle willen houden en voorzichtige burgers die hetzelfde willen doen met hun persoonlijke gegevens. In beide gevallen kunnen DRM technieken een bijdragen leveren, maar vooral in situaties waarin de gebruikers goedwillend zijn. Door DRM software zouden ze dan gewaarschuwd kunnen worden op het moment dat ze mogelijk de fout in gaan: *hang on, you probably don't want to do this!* Fatsoenlijke organisaties zullen zich waarschijnlijk wel aan de regels willen houden, al was het alleen maar om aansprakelijkheid en imagoschade te voorkomen.

Beheer van gegevens

Bij het beheer van gevoelige digitale (persoons)gegevens spelen drie aspecten een rol.

1. Wie heeft de 'orginele' gegevens in bezit? Het woord originele staat hier tussen haakjes omdat bij digitale er geen onderscheid gemaakt kan worden tussen een

origineel en een kopie. Waar het hier vaak om gaat is vooral wie kan authentieke (vers ondertekende) kopieën verstrekken?

2. Wie bepaalt de policies / gebruiksregels voor die gegevens?

3. Hoe weet men zeker dat anderen zich houden aan die policies?

Indien ik controle wil houden over mijn persoonsgegevens kan dat in principe op drie manieren.

a. Ik ben degene die alle originele gegevens in handen heeft; ik verstrek die gegevens[2] alleen aan partijen die ik vertrouw (in de zin dat ze zich houden aan de policies die ik eraan meegeef). Met name deze aspecten worden later verder uitgewerkt in Hoofdstuk 21.

b. Ik heb niet de originelen in handen, maar ben wel degene die de bijbehorende *sticky* policies bepaalt. Dit laatste werkt alleen in een omgeving waar alle anderen zich aan die bijbehorende policies houden.

c. Ik heb noch over de originele gegevens noch over de bijbehorende policies controle, maar ik bepaal wel wanneer de gegevens aan een (deel-)identiteit van mij gekoppeld worden.

Al deze posities zijn in zekere zin naïef en op dit moment niet realistisch. De bank of belastingdienst zal niet alle gegevens over mij in mijn handen willen geven, en zal mij ook niet de policies over mijn gegevens laten bepalen. Voor een aantal van hun bedrijfsprocessen is het cruciaal dat ze zelf controle over (een deel van) de gegevens over mij hebben. Toch hanteren ze wel degelijk meer of minder expliciete policies in de behandeling van gegevens. Het is voor hen belangrijk het vertrouwen van de klanten niet te schaden. Het is me echter niet zo duidelijk hoe sterk het besef bij zulke organisaties aanwezig is dat klanten mogelijk invloed zouden willen (en kunnen) hebben op die policies.

De gegevens zouden binnen organisaties wel in hoge mate geanonimiseerd behandeld kunnen worden, waarbij alleen op een beperkt aantal momenten een koppeling tussen een interne en externe identiteit plaatsvindt: waarom moet altijd mijn naam gekoppeld worden aan mijn banknummer, bijvoorbeeld op een bankpas? En waarom krijg ik van mijn bank voor een elektronische betaling niet iedere keer een tijdelijk rekeningnummer dat alleen voor die transactie gebruikt wordt?

Op termijn is het van belang een werkbare combinatie van bovenstaande drie opties te ontwikkelen.

[2] Een mogelijkheid is ook dat ik niet de gegevens zelf vertrek, maar een gepersonaliseerde link of pointer ernaartoe, zodat de ontvanger altijd de meest actuele versie kan opvragen en ik de verstrekking weer ongedaan kan maken. Dit werkt alleen in een omgeving met zeer betrouwbare netwerken en met partijen die zich aan de regels willen houden.

Hoofdstuk 13

Biometrie en identiteitsdocumenten

In Hoofdstuk 4 is al kort over biometrie gesproken. Het paspoort en de nationale identiteitskaart bevatten in Nederland sinds kort een chip met daarop biometrische gegevens van de houder. Vooralsnog gaat het om een digitale gelaatsfoto, maar halverwege 2009 zullen ook een digitale versie van de afdrukken van de twee wijsvingers opgenomen worden. Praktisch iedereen zal dus met biometrie te maken krijgen. Daarom is het de moeite waard iets dieper op het onderwerp in te gaan, met name in relatie tot identiteitsdocumenten.

Bij het gebruik van biometrie worden lichaamseigen kenmerken opgemeten en gebruikt als bewijs van identiteit (authenticatie). Bij het opmeten leidt zo'n kenmerk, bijvoorbeeld een vingerafdruk, tot een digitale representatie, die ook wel *template* genoemd wordt. Biometrie kan op twee fundamenteel verschillende manieren gebruikt worden.

- **Biometrische verificatie**. Hierbij heeft de controleur een bekende template voorhanden en wordt van een onbekende persoon nagegaan of het toevallig zijn of haar template is. Eerst wordt die persoon (biometrisch) gemeten, en vervolgens wordt de resulterende 'verse' template vergeleken met de voorhanden template. Zijn die twee hetzelfde (binnen bepaalde marges), dan is er sprake van een match en is de identiteit van de persoon geverifieerd. Zo niet, dan is men nog niet veel wijzer.

  Deze verificatie-vorm van biometrie wordt gebruikt bij het nieuwe paspoort. In de chip van het paspoort staat een 'oude' template die voorzien is van een digitale handtekening door de Nederlandse staat[1]. Bij een grenspassage wordt deze geauthoriseerde template uit de paspoortchip gelezen en vergeleken met een verse template van de passerende persoon. Op zo'n manier kan gecontroleerd worden of het paspoort wel echt bij die persoon hoort, en wordt zogenaamde *look alike* fraude tegengegaan.

[1] Dit gebeurt in feite indirect: op de template staat een handtekening van de producent van het paspoort (SDU), maar voor die producent is er weer een certificaat dat getekend is door de staat.

- **Biometrische identificatie**. Hierbij beschikt de controleur over een databank van bekende templates, en is het de bedoeling de identiteit van een onbekende persoon vast te stellen door een verse template van die persoon te vergelijken met alle beschikbare templates in de databank. In het geval dat er een match optreedt is de identiteit vastgesteld.

  Deze methode wordt bijvoorbeeld toegepast wanneer er bij een misdrijf op de plaats van het delict sporen van DNA of vingerafdrukken worden aangetroffen. De politie kan daarmee op zoek gaan in haar databanken van bekende, eerder veroordeelde personen. Ook kan zo'n lijst van templates gebruikt worden om bijvoorbeeld mensen met een stadion- of zwembad-verbod te identificeren, en bij identificatie de toegang te weigeren. De databank fungeert dan als een *black list*.

Bij verificatie is dus sprake van één enkele vergelijking (van templates), terwijl het bij identificatie typisch om veel meer vergelijkingen gaat. Voor identificatie is dus meer rekenkracht en tijd nodig. Het kan *real-time* alleen met betrekkelijk kleine databanken.

Templates vormen identiteitsbewijzen en dienen daarom goed beschermd te worden. Misbruik kan ernstige gevolgen hebben, bijvoorbeeld wanneer iemand onterecht verantwoordelijk gehouden, of zelfs veroordeeld, wordt. Templates kunnen het in meer of mindere mate mogelijk maken het origineel te reconstrueren. De vingerafdruk templates in het paspoort zijn bijvoorbeeld gewoon jpeg plaatjes. Hiermee is makkelijk een nepvinger te maken. Voor DNA-templates is zoiets minder voor de hand liggend, maar niet onmogelijk.

Het grote probleem bij biometrie is dat de gebruikte lichaamskenmerken onvervangbaar zijn: een nieuwe (andere) vingerafdruk kun je niet zomaar bestellen. Wachtwoorden zijn een andere vorm van identiteitsbewijzen, waarbij er twee gouden regels zijn: verander je wachtwoord regelmatig, en gebruik hetzelfde wachtwoord nooit op twee verschillende plaatsen—de beheerder op de ene plaats kan je wachtwoord afvangen en misbruiken op de andere plaats om zich als jou voor te doen. Bij biometrie breek je deze beide regels op overduidelijke wijze—je gebruikt immers altijd en overal dezelfde vinger—en maak je jezelf daardoor kwetsbaar. Een ander groot probleem is dat men bij iedere applicatie lijkt te denken de enige te zijn die gebruikt maakt van de gekozen vorm van biometrie. Maar iedereen wil plotseling biometrie introduceren—voor fun en voor security—waardoor onvoorziene en ongewenste interferentie kan ontstaan. In Nijmegen is er bijvoorbeeld een coffeeshop die vingerafdrukken gebruikt om geregistreerde klanten (van boven de 18) te herkennen. Als vervolgens diezelfde vingerafdruk wordt gebruikt voor toegang tot je bankrekening kan er een probleem ontstaan: de coffeeshophouder kan nepvingers gaan maken en daarmee bankrekeningen plunderen.

Naast problemen met de onvervangbaarheid van biometrie zijn er ook problemen met de inherente foutmarges. Die marges verschillen per vorm van biometrie, maar ze zijn nooit nul. Er worden ook daadwerkelijk fouten mee gemaakt, met soms erg onaangename consequenties. De Amerikaanse jurist Brandon Mayfield werd verdacht van betrokkenheid bij de grote bomaanslagen in Madrid van maart 2004 op basis van

een vingerafdrukvergelijking. In mei 2004 zat hij daarom bijna twee en halve week vast. Achteraf bleek er sprake van grote fouten bij de vergelijking en is zo'n 2 miljoen dollar aan compensatie uitbetaald.

Hoe biometrie organiseren?

De inzet van biometrie kan misschien bedoeld zijn om identiteiten met zekerheid vast te stellen, maar een ondoordacht beheer ervan kan juist het risico op identiteitsfraude vergroten. Hoe moeten we dat gebruik van biometrie dan organiseren? Er zijn ruwweg drie methoden.

In het eerste geval worden biometrische gegevens in een centrale databank opgeslagen en vindt iedere vergelijking plaats op basis van de templates in die databank. Dit is de slechtst mogelijke opzet. Insiders kunnen op ieder moment makkelijk een template selecteren en misbruiken voor identiteitsfraude. En wanneer kwaadwillende hackers zich op de databank richten kan de gehele inhoud op straat komen te liggen. Op dat moment kan van iedereen de identiteit nagemaakt worden en leidt een infrastructuur die oorspronkelijk bedoeld was om identiteiten beter vast te stellen tot grootscheepse ondermijning van die doelstelling—zonder de mogelijkheid van herstel; lichaamskenmerken zijn immers onvervangbaar.

In het tweede geval worden (geautoriseerde) templates aan de dragers ervan meegegeven, zoals bij het biometrische paspoort. Dan is er geen centrale databank meer nodig, waardoor ook de mogelijkheid van identificatie vervalt. Het gaat in dit geval om verificatie. Dit is al een stuk veiliger, maar het grote risico dat overblijft is dat bij metingen de biometrische gegevens aan een onbekend leesapparaat afgegeven moeten worden. Het risico zit hier in de apparatuur. Bij iedere vingerafdruklezer, of iedere andere biometrische opnemer, is het onduidelijk wat er met de opgenomen verse templates gebeurt. Het mag dan de bedoeling zijn dat de opgenomen template enkel vergeleken wordt met de meegebrachte template, maar of die template dan niet stiekem ook alsnog in een grote databank opgeslagen wordt is onduidelijk. Het is zeer waarschijnlijk dat allerlei landen de vingerafdruklezers voor paspoortcontrole aan hun buitengrenzen direct koppelen aan een grote databank om alle opgenomen templates van binnenkomende reizigers op te slaan. Iedere biometrisch uitlezing introduceert aldus een risico op identiteitsfraude. Indien je veel reist, en dus ook vaak je vingerafdrukken in allerlei landen achterlaat kun je er maar het beste van uit gaan dat je vingerafdrukken op straat liggen: voor *high-level security* zijn ze niet meer bruikbaar.

In het derde geval heeft het individu niet alleen de geautoriseerde template bij zich, maar ook een geautoriseerde lezer en vergelijker van templates. Indien verificatie van de identiteit van een persoon gewenst is geeft die persoon zijn biometrische gegevens af aan de eigen lezer, waarna de eigen vergelijker vaststelt of er sprake is van een match met de meegebrachte geautoriseerde template. De controlerende partij kan bij een positieve uitkomst tevreden zijn omdat het om geautoriseerde apparatuur gaat.

Dit laatste scenario—zie ook Hoofdstuk 21—mag in eerste instantie vreemd klinken, maar is in feite niet zo onredelijk vanwege het kleinste risico op misbruik van bio-

metrische templates. Deze gedecentraliseerde aanpak bestaat al wel in andere contexten, zoals bij memory sticks met geïntegreerde vingerafdruklezer voor authenticatie. Ook kan men zich voorstellen dat een vingerafdruklezer, of een andere biometrische lezer, opgenomen wordt op een chipkaart, in een GSM, in een handcomputer, of in andere persoonsgebonden apparaatjes met beveiligde afgeschermde hardware. Ook hier wordt al aan gewerkt, bijvoorbeeld bij een GSM die geactiveerd wordt na biometrische verificatie op basis van de maten van de oorschelp van de eigenaar.

Biometrie kan een nuttig mechanisme zijn, maar de mogelijkheden worden snel overschat. Biometrie moet met zorg gebruikt worden, in het volle bewustzijn van de bijbehorende beperkingen en risico's. Terughoudendheid in het gebruik is vereist, waarbij een zo groot mogelijke decentralisatie—van templates en van apparatuur voor uitlezen en vergelijken daarvan—het risico op identiteitsfraude door misbruik van templates minimaliseert. En reductie van identiteitsfraude is waar het uiteindelijk allemaal om draait.

Hoofdstuk 14

RFIDs

De afkorting RFID staat voor *Radio Frequency Identification*. Het gaat hierbij om kleine computerchips die op verzoek identificerende informatie uitstralen. Soms zitten de chips in een plastic kaartje van credit card formaat, maar soms ook in een nauwelijks zichtbaar plakkertje of korreltje. De meeste eenvoudige, zogenaamde passieve, RFIDs hebben geen batterij als voeding maar een kleine antenne die een geschikt elektromagnetisch signaal omzet in een stroompje waarmee de chip eventjes gaat werken en direct een eigen nummer terugstuurt, mogelijk met nog wat extra informatie. Zulke RFID-chips kunnen bijvoorbeeld in bibliotheekboeken geplakt worden. Bij de uitleenbalie is het dan genoeg de boeken over een scanner te halen zodat het nummer van de RFID-chip (en daarmee het boek) gekoppeld kan worden aan de uitlener. Niet alleen objecten maar ook dieren en soms zelfs mensen worden voorzien van RFID-chips. Het is de moeite waard in de context van identificatie daar nader bij stil te staan.

Voor grote organisaties, zoals supermarkten, is het geen kleinigheid om zicht te houden op alle spullen die ze in huis hebben. Het gaat dan niet alleen om wat er in de winkel ligt, maar ook in de voorraadschappen, om wat er snel of traag verkocht wordt, en om wat er bij een kassa voorbijkomt. Traditioneel worden steepjescodes (ofwel *barcodes*) gebruikt om artikelen te herkennen. Meestal gaat het dan echter alleen om het soort artikel (zoals scheermesjes), en niet om individuele artikelen: verschillende losse pakjes van dezelfde soort scheermesjes hebben dezelfde code. Een ander nadeel is dat streepjescodes handmatig met een scanapparaatje uitgelezen moeten worden: aan de kassa moet in principe ieder item afzonderlijk langs de barcodelezer gehaald worden, resulterend in het welbekende piepje. Je kunt die omslachtige uitlezing echter ook als een voordeel zien.

Indien individuele artikelen van een eigen RFID-chip voorzien worden is er meer mogelijk. De chips zijn van afstand uitleesbaar, vaak vanaf enkele meters, met meerdere items tegelijkertijd. Zo kun je met een vol boodschappenwagentje in één keer langs de kassa rijden zonder dat de losse artikelen één voor één op de band gelegd en gescand hoeven te worden. Daarvoor is het nodig om artikelen individueel te *taggen* (van een RFID-chip voorzien) om te kunnen herkennen of u nu één of tien pakjes condooms meeneemt. Ook kan het beheer van de *supply chain* verbeteren doordat er

gedetailleerd zicht op alle individuele artikelen mogelijk is. Dat vereist echter ook een erg goed doordacht informatiebeheer omdat de informatiestroom dramatisch toeneemt en om een overzichtelijke presentatie vraagt. De Amerikaanse supermarkt *Wal-Mart* is ver gevordered met het gebruik van RFID, en legt het gebruik van zulke chips op aan alle toeleveranciers. Zo'n grootschalige inzet van deze nieuwe technologie is mogelijk omdat de prijs van individuele chips erg laag geworden is, tot onder de vijf cent. Die prijs kan nog verder dalen door de introductie van 'plastic' chips.

Behalve artikelen kunnen ook levende wezens voorzien worden van RFID-chips, bijvoorbeeld via implantatie. Bij vee kan op zo'n manier beter zicht gehouden worden op vervoersbewegingen, zeker op het moment dat er een uitbraak plaatsvindt van een besmettelijke ziekte. Met bij mensen geïmplanteerde RFID-chips zijn ook allerlei leuke en minder leuke toepassingen mogelijk. Bekend is de Baja Beach Club in Rotterdam die toegang en afrekening op basis van identificatie met geïmplanteerde chips mogelijk maakt. De chip die bij vrijwilligers in de arm geschoten wordt zendt een specifiek getal als identificatie uit, waardoor in een computersysteem de bijbehorende naam en het resterende krediet opgezocht kunnen worden. Een iets minder ingrijpend gebruik komt voor in ziekenhuizen waar patiënten bij binnenkomst een polsbandje met RFID chip krijgen zodat ze makkelijker herkend en getraceerd kunnen worden.

Implantatie van RFID-chips is voor veel mensen een eng idee. Af en toe roept een overspannen bestrijder van terrorisme of criminaliteit dat we iedereen een chip in de nek moeten schieten. Vooralsnog biedt artikel 11 van de grondwet daar bescherming tegen: ieder heeft, behoudens bij of krachtens de wet te stellen beperkingen, recht op onaantastbaarheid van zijn lichaam. Een iets minder ingrijpende oplossing is om mensen chipkaarten te geven met daarin een RFID-chip. Dit vindt bijvoorbeeld plaats bij het biometrische paspoort en bij de OV-chipkaart. Bij het paspoort wordt de koppeling tussen persoon en chip gelegd via biometrie, en niet via implantatie. De OV-kaart is wel overdraagbaar, maar vertegenwoordigt waarde, zoals de chipknip, waardoor overdracht geremd wordt. Maar natuurlijk kan er onderling mee afgerekend worden: "ik kan je nu niet betalen, maar neem mijn OV-chip maar; daar staat nog 50 Euro op; de rest krijg je nog wel." Profielboeren houden daar echter niet van.

Misbruik

Het moge duidelijk zijn dat je met RFID technologie leuke en nuttige dingen kunt doen. Maar ook minder leuke. De meeste RFID-chips zijn van de goedkoopste 'domme' soort die direct hun identiteit prijsgeven aan wie het ook maar vraagt. Iedereen kan ze ongemerkt uitlezen (*skimmen*). Nou lijkt dat misschien veel minder erg bij dingen (objecten) dan bij mensen (subjecten), maar als mijn horloge, portemonnaie of OV-chipkaart—of iets anders dat ik bijna altijd bij me heb—zo'n chip bevat ben ik toch vrij makkelijk overal te herkennen aan de bijbehorende nummers—en dus traceerbaar.

Er bestaat een haast onbedwingbare neiging—vaak met de beste bedoelingen—om van alles en nog wat van RFID-chips te voorzien, zoals fietsen (tegen diefstal) en autonummerplaten (tegen fraude of voor efficiënte verkeerscontrole). Maar door al dat

soort maatregelen kunnen we elkaar onderling steeds intensiever gaan traceren.

Laagdrempelige traceerbaarheid is een probleem. Velen van ons zijn ook traceerbaar via de locatiegegevens van onze mobiele telefoons. Die gegevens worden geregistreerd door GSM masten en (steeds minder[1]) tijdelijk opgeslagen in de databanken van de telecommunicatie maatschappijen. Ze zijn niet algemeen toegankelijk. Behalve de maatschappijen zelf kunnen hooguit inlichtingen- en opsporings-diensten er onder (steeds minder) speciale omstandigheden inzicht in krijgen. Traceerbaarheid via GSMs is dus voorbehouden aan een beperkt aantal 'officiële' partijen. Daartegenover kan iedereen een RFID lezer kopen, aan zijn of haar laptop koppelen en daarmee de RFID-chips in de direct omgeving registreren en volgen.

Deze democratisering van de traceerbaarheid kan ingrijpende gevolgen hebben voor de persoonlijke veiligheid. Stalking wordt er een stuk eenvoudiger mee. Er zal een informele markt ontstaan van RFID gegevens. Een inbreker zou er gebruik van kunnen maken door van buitenaf een huis vooraf te scannen op aanwezigheid van waardevolle artikelen. Het zou ook niet best zijn wanneer het nummer van de RFID-chip in het horloge van de minister president op het internet verscheen. Kwaadwillenden kunnen dan een bom maken die alleen afgaat wanneer dat nummer in de omgeving verschijnt. Maar hetzelfde geldt natuurlijk voor de RFID in de nummerplaat (of in de fiets, etcetera) van de minister president. In feite gelden zulke risico's voor ons allemaal. Het is zaak hier beter bij stil te staan voordat er grote ongelukken gebeuren.

Naast het *skimmen* van een RFID-chip kan men ook *clonen*: de verkregen gegevens in een andere chip zetten. Natuurlijk kan men ook de gegevens iets wijzigen voordat ze in een andere chip geplaatst worden. Daarmee kan identiteitsfraude gepleegd worden, of kunnen organisatorische zaken behoorlijk in de war geschopt worden, zodat bijvoorbeeld artikelen met aangepaste prijzen meegenomen worden.

Er wordt inmiddels ook gewerkt aan beschermingsapparaatjes tegen RFID[2]. Zulke apparaatjes verstoren de communicatie tussen RFID-lezer en chip, waardoor chips zeer selectief (of geheel) onzichtbaar gemaakt kunnen worden. Misschien moeten we allemaal met zo'n *guardian* rond gaan lopen. Maar het is natuurlijk ook verleidelijk zo'n ding in je volle kar met boodschappen te stoppen, zodat bij het passeren van de kassa een deel van de lading helemaal niet zichtbaar is en dus ook niet betaald hoeft te worden.

We zullen ons goed bewust moeten zijn van de risico's van RFID-chips in het algemeen, en van de domme varianten die enkel hun identiteit uitstralen in het bijzonder. Waarschijnlijk zijn deze domme chips alleen inzetbaar in onschuldige situaties waarbij er geen financiële waarde of persoonlijke identiteiten in het geding zijn. Men kan er te eenvoudig mee frauderen. Een zekere mate van cryptografische afscherming is nodig voor serieuze toepassingen. Wanneer identiteiten in het geding zijn is het bijvoorbeeld redelijk om de zaak zo in te richten dat de omgeving zich eerst moet authenticeren en

[1] Door verandering van wettelijke eisen.

[2] Bijvoorbeeld aan de Vrije Universiteit van Amsterdam, zie `www.rfidguardian.org`.

dat de chip alleen reageert op geauthenticeerde lezers. Dit vergt echter ingewikkeldere en dus ook duurdere chips. Om de markt ertoe te bewegen zulke chips te gebruiken zal enige aanmoediging of zelfs wettelijke dwang nodig zijn.

Regelgeving

Een fundamenteel probleem bij RFID-chips is dat ze zo klein zijn dat je ze moeilijk opmerkt. Daar komt dan nog bij dat de communicatie draadloos verloopt zodat mensen ongemerkt uitgelezen en gevolgd kunnen worden via de chips die ze bij zich dragen. Dat is inderdaad zorgwekkend. Inmiddels is er dan ook een beweging op gang gekomen die pleit voor (zelf)regulering waarbij uitgangspunt is dat bekend moet zijn of een product een RFID-chip bevat, en zo ja waar, wanneer en waarom welke informatie uitgelezen wordt. Verder zou de chip op verzoek (na aankoop) vernietigd moeten worden. Natuurlijk kun je dat ook zelf doen door je aankoop met de chip thuis in de magnetron te leggen. Echter, bij sommige artikelen, zoals horloges, is dat misschien niet verstandig. Een deel van de genoemde uitgangspunten wordt al geregeld door de Wet Bescherming Persoonsgegevens (Wbp).

Aanpassing of aanvulling van de bestaande wetgeving lijkt toch noodzakelijk, bijvoorbeeld om notificatie en vernietiging duidelijk te regelen, of om het strafbaar te stellen dat iemand heimelijk gevolgd wordt via RFID. Deze situatie kan vergeleken worden met de recente strafbaarstelling van heimelijk cameratoezicht, als gevolg van het op de markt verschijnen van goedkope webcams en mobieltjes met cameras.

Interessant is de zorg in christelijke kringen over het gebruik van RFID-chips voor persoonlijke identificatie. Hiertegen bestaan principiële bezwaren op basis van een bijbeltekst waarin gesproken wordt van de komst van een kwade macht (het beest) die iedereen van een merkteken voorziet[3]. RFID-gebruik zou een voorbode van deze komst zijn. Binnen de Nederlandse politiek heeft de Christen Unie tot nu toe zich het meest serieus met het onderwerp RFID bezig gehouden, via een eigen nota[4] van de parlementaire fractie in mei 2005. Ook daarin wordt aangedrongen op aanvullende wetgeving. Meer in het algemeen valt op dat zorg om privacy leeft in de protestante gemeenschap die natuurlijk traditioneel sterk gericht is op (“gedecentraliseerde”) individuele geloofsbelevenis en persoonlijke autonomie.

[3] Openbaring 13:16: Verder liet het bij alle mensen, jong en oud, rijk en arm, slaaf en vrije, een merkteken zetten op hun rechterhand of op hun voorhoofd.

[4] Beschikbaar via `www.christenunie.nl`.

Deel IV

De overheid

Hoofdstuk 15

Big Brother en Soft Sister

De overheid heeft in onze samenleving een aantal monopolies, waaronder bijvoorbeeld het geweldsmonopolie. Maar ook op het gebied van identiteiten is er een overheidsmonopolie, namelijk op het scheppen en uitgeven van zogenaamde bronidentiteiten. Natuurlijk kan ik ook een identiteitsdocument hebben van andere organisaties, zoals een lidmaatschapskaart van de tennisclub. Maar zo'n document is van een andere orde dan mijn paspoort. De overheid vormt de bron en creëert de middelen waarop teruggevallen kan worden. Ze zijn zelf niet weer op andere documenten gebaseerd.

Naast deze creatietaak heeft de overheid ook nog een taak met betrekking tot het beheer van identiteiten en attributen—bijvoorbeeld in de Gemeentelijke Basis Administratie (GBA)—en tot de controle—bijvoorbeeld bij grensovergangen. Voor dit alles gebruikt de overheid een eigen infrastructuur voor identiteiten.

De overheid kent een grote verscheidenheid aan organen. Alleen op een abstract niveau is er sprake van een eenheid. Hier onderscheiden we twee belangrijke rollen, namelijk 'Big Brother' waarbij de overheid het minder vriendelijke, controlerende gezicht aan de burgers laat zien, en 'Soft Sister' waarbij de nadruk ligt op vriendelijke dienstverlening. Deze twee rollen worden later in dit hoofdstuk nader uitgewerkt. Ze lijken op gespannen voet te staan, maar blijken toch verrassend goed, en misschien wel steeds beter, samen te kunnen gaan. Natuurlijk is dat wel enigszins afhankelijk van de invulling van het begrip 'dienst'.

Binnen deze twee rollen zelf zijn er ook spanningsvelden. Binnen de Big Brother context zijn er enerzijds klachten over de onveiligheid. Maar wanneer de overheid daar echt wat aan gaat doen piept de burger snel dat hij of zij zo vaak gecontroleerd wordt. Binnen de Soft Sister context zijn er aan de ene kant klachten wanneer er alweer een uitvoerig formulier ingevuld moet worden, maar wordt er aan de andere kant geprotesteerd wanneer blijkt dat de overheid zoveel al weet over haar burgers.

De grote vraag hierbij is altijd: wat wil de burger zelf, in het algemeen of individueel[1]? Op die vraag komt zelden een duidelijk antwoord. Het is verleidelijk te gaan roepen "de burger wil dit" of "de burger wil dat", maar deugdelijk onderzoek

[1] Bij een overzichtelijke individuele variëteit kunnen gepaste keuzemogelijkheden geschapen worden.

ontbreekt meestal. Wat wel opvalt is dat burgers in Nederland ondanks alles een groot vertrouwen in de overheid lijken te hebben. Dat valt zeker op wanneer je de situatie hier vergelijkt met die in Amerika. Daar treft men een wantrouwen jegens overheidsbemoeienis aan dat dieper geworteld en wijder verspreid is dan wij gewoon zijn. Dit ondanks de eigen historische ervaringen met kwaadwillende overheden, zoals gedurende 1940–1945 toen effectief en dankbaar gebruik gemaakt werd van de uitstekende identiteitsinfrastructuur, met name voor de vervolging van Joden.

Misschien wel onze belangrijkste sociale verworvenheid is de rechtsstaat waarin we leven. Een wezenlijk kenmerk daarvan is dat de overheid niet alles mag, en zelf ook aan regels gebonden is. Het is een groot goed dat de politie niet zomaar je huis mag binnenvallen en dat rechters onafhankelijk zijn en voor de overheid onaangename beslissingen kunnen nemen, bijvoorbeeld in door individuele burgers aangespannen processen. Zo'n proces aanspannen zou je in een dictatuur wel uit je hoofd laten. Ondanks al het bestaande, al of niet terechte, vertrouwen in de overheid is terughoudendheid gepast in het toekennen van macht aan de overheid. Sterker nog, een zekere mate van wantrouwen is zeer gezond. Het is wezenlijk dat er sprake is van een redelijke machtsbalans tussen burgers en overheid.

Onder druk van terrorisme is duidelijk dat de overheid de laatste jaren de eigen burgers, en vooral ook de bezoekers van buiten, minder vertrouwt. Ze worden aan strengere controlemechanismen met betrekking tot hun identiteit en attributen onderworpen. In zo'n context is het volstrekt redelijk om ook andersom de burgers meer rechten en middelen in handen te geven om organisaties met wie ze te maken hebben om authenticatie te vragen voordat er tot overdracht van allerlei gevoelige gegevens overgegaan wordt. In het bijzonder betekent dit dat de ICT-systemen die ons steeds indringender omringen zich nadrukkelijk eerst moeten kunnen authenticeren. Om de resulterende authenticaties, typisch met certificaten, te kunnen controleren moeten burgers zelf ook controlemiddelen in handen hebben. Daar komen we in Hoofdstuk 21 op terug.

Soft Sister: gemak of privacy?

De overheid heeft zich de laatste jaren het nobele doel gesteld de dienstverlening aan de eigen burgers te verbeteren[2]. ICT, en met name het internet, moet daarbij een belangrijke rol spelen. De eerste stappen van de overheid op dat gebied kunnen gekenschetst worden als de fase van de omgevallen boekenkast. Zo ongeveer alle informatie voor burgers is op websites van de overheid gedumpt. Dat maakt veel van die informatie makkelijker toegankelijk, en sneller te vinden, bijvoorbeeld via zoekmachines. Dat is allemaal positief.

In die omgevallen kasten zitten ook veel formulieren. Die kan de burger zelf thuis afdrukken en invullen, om daarna het traditionele interactieproces mee te doorlopen:

[2]Zie bijvoorbeeld het actieprogramma 'Andere Overheid' uit 2003, beschikbaar via `www.andereoverheid.nl`.

persoonlijk afgeven aan het loket waarbij traditionele authenticatie plaatsvindt. Om ook zulke interacties elektronisch te laten verlopen moet de overheid de burger aan de andere kant van de lijn met zekerheid kunnen herkennen, bijvoorbeeld bij de aanvraag van verlenging van het rijbewijs. Dit is een belangrijke motivatie om de infrastructuur voor het beheer van identiteiten uit te breiden, bijvoorbeeld met DigiD.

Een van de punten waar men zich in vastgebeten heeft is het principe van eenmalige gegevensverstrekking. Dat betekent dat aan burgers geen gegevens meer gevraagd (mogen) worden die al binnen de overheid beschikbaar zijn. Dit klinkt redelijk maar betekent in feite dat compartimentalisatie van gegevens binnen de overheid onder druk komt te staan, terwijl dat toch een van de basisprincipes van privacyvriendelijk gegevensbeheer is: scheiding van rollen en van bijbehorende gegevens. Alle informatie over mij binnen de overheid moet overal waar ze nodig zou kunnen zijn ook daadwerkelijk beschikbaar zijn. De implementatie daarvan is niet triviaal. De meest voor de hand liggende (en meest kwetsbare) oplossing is om een centrale databank op te richten met daarin alle gegevens die de overheid over mij heeft. Een alternatief is om meerdere databanken op te zetten met allemaal deelgegevens over mij. Deze laatste aanpak klinkt beter maar is ook gecompliceerd. Een zeer zorgvuldige omgang met autorisaties is vereist: mag afdeling A die gegeven X over mij heeft deze X ook doorgeven aan afdeling B? Mag afdeling B een locale copie van X bewaren? Zijn dit soort zaken allemaal goed doordacht en vastgelegd in heldere regels? Kan ik ervan uitgaan dat de overheid onder dit zelf opgelegde regime van eenmalige gegevensverstrekking de resulterende complexiteit aankan en zorgvuldig met mijn gegevens om zal gaan? Of betekent dit dat alle gegevens over mij binnen de overheid zeer gemakkelijk gekoppeld worden. De gedachtengang achter het BSN en deze eenmalige gegevensverstrekking lijkt te zijn dat de overheid nog maar één rol van mij accepteert, en geen onderscheid meer wil maken tussen mij zeg als belastingbetaler en als snelheidsovertreder.

Het belangrijkste mechanisme voor de realisatie van deze eenmalige gegevensverstrekking is het Burger Service Nummer (BSN). Door alle gegevens over mij binnen de overheid (en gedeeltelijk ook daarbuiten) aan mijn BSN te koppelen zijn ze makkelijker te herkennen en te delen. Op basis van mijn BSN kan de hele lijst met gegevens die mij betreffen te voorschijn komen. Het BSN maakt mij transparant. Het rijgt allerlei rollen aaneen die ik zelf misschien wel gescheiden wil houden. Toch wordt dit BSN eufemistisch gepresenteerd als een 'service'. Maar voor wie? De Raad van State heeft nadrukkelijk opgemerkt dat het vooral gaat om service voor de overheid zelf, en niet voor de burger[3].

In Amerika worden persoonlijke nummers als van credit card of *social security*

[3]In het advies van 1 juli 2005, zie §§2: "Het zijn echter vooral de overheid en de bedrijven die betrokken zijn bij de uitvoering van overheidsregelingen die profijt zullen hebben van dit gebruik. De positie van de burger komt in het wetsvoorstel, anders dan als object, niet aan de orde. . . . Van rechten van de burger is ook weinig sprake. Daarom verbaast het de Raad dat gekozen is voor de benaming 'burgerservicenummer'; een meer neutrale aanduiding als 'algemeen registratienummer' of iets dergelijks ligt naar zijn oordeel meer voor de hand. De Raad adviseert een neutrale, niet-suggestieve term te gebruiken voor dit persoonsnummer."

grootschalig gebruikt voor identiteitsfraude. Brede invoering van het BSN maakt zo'n nummer ook bij ons aantrekkelijk voor fraudeurs, omdat er zoveel mee kan. Ondanks alle goede (naïeve) bedoelingen zal ons dat ook te wachten staan. Het als 'service' gepresenteerde nummer confronteert de burger met nieuwe risico's.

Op basis van alwetendheid door koppelingen via het BSN kan de overheid zich zelfs in de positie van de burger verplaatsen en pro-actief voor die burger gaan denken en handelen. Met enige ironie zou men hierin een vorm van identiteitsfraude kunnen zien. De overheid weet meer dan voldoende om te zien of ik recht heb op huursubsidie, en kan het in dat geval dan ook maar beter voor mij aanvragen. Ook belastingformulieren kunnen grotendeels al door de overheid ingevuld worden. U hoeft alleen nog maar te tekenen. En misschien hoeft die ondertekening binnenkort ook niet meer.

Zitten we hier werkelijk op te wachten? Het is een vorm van goedbedoelde overheidsbemoeienis en inmenging waar ik jeuk van krijg. De overheid gaat er van uit dat wij omwille van enig gemak voor ons—en heel veel gemak voor zichzelf—wel een deel van onze privacy op willen offeren. Maar is er wel goed over nagedacht of dit een of-of kwestie is? Ik wil èn gemak èn privacy! Deze combinatie lijkt uitgesloten in de centralistische gedachtenwereld waarin de overheid vastgeroest zit.

Het met de hand invullen van lange formulieren is inderdaad vervelend. Maar als we onze ICT infrastructuur decentraal inrichten op een manier waarbij mensen zelf over hun eigen (elektronische) gegevens beschikken kan dit invullen gebeuren met een paar drukken op de knop. In zo'n scenario zou ik voor het elektronisch invullen van een formulier een aantal relevante gegevens op mijn eigen handcomputer (zie Hoofdstuk 21) kunnen selecteren en koppelen aan door mij gekozen gebruiksregels (de *policy*) om ze vervolgens—na geslaagde wederzijdse authenticatie—aan de betreffende overheidsdienst te geven. Dit garandeert zowel privacy als gemak. Dat laatste is misschien niet direct duidelijk voor de huidige generatie, maar waarschijnlijk wel voor de volgende.

Bij deze overdracht geldt natuurlijk, zoals opgemerkt in Hoofdstuk 11, dat veel interacties kunnen plaatsvinden op basis van attributen en niet noodzakelijk op basis van identiteiten. Hoe zuiniger de overdracht hoe kleiner het risico op identiteitsfraude.

Big Brother: veiligheid of privacy?

Een van de centrale taken van de overheid is te zorgen voor de veiligheid van burgers, bijvoorbeeld door het bouwen van dijken, opstellen van bouwvoorschriften, vervolgen van criminelen, enzovoort. Belangrijke onderdelen daarbij zijn risicoanalyse, normstelling en handhaving. Voor die handhaving is de overheid enerzijds afhankelijk van tips en aangiften van anderen, en anderzijds van eigen monitoring en controle van wat daadwerkelijk plaatsvindt. Dit laatste aspect heeft de laatste jaren nadrukkelijk meer aandacht gekregen, onder druk van terrorisme.

Bij risicoanalyses worden koele berekeningen gemaakt die vertellen dat eens in de zoveel jaar dijken breken en tunnels of bruggen instorten, met een inschatting van het bijbehorende verlies aan mensenlevens. Analyse en ervaring van risico's zijn echter

heel verschillende zaken. Vliegen is als middel van vervoer veel veiliger dan autorijden maar velen ervaren dat anders. Op een vergelijkbare manier is terrorisme tot op dit moment niet zo'n heel grote bedreiging. Technisch gezien kunnen we het tot nu toe goed aan, en is het aantal slachtoffers relatief gering—in vergelijking met bijvoorbeeld kindermishandeling, waardoor jaarlijks in Nederland zo'n vijftig kinderen overlijden. Dat is vaak hartverscheurend maar krijgt veel minder aandacht. En op de een of andere manier zijn we ook niet bereid er veel meer middelen voor in te zetten of ingrijpende maatregelen tegen te nemen die de privacy en autonomie van ouders aantasten. Zo'n bereidheid in te grijpen tegen terrorisme betaat wel, maar de middelen en maatregelen die we ertegen inzetten zijn feitelijk niet geheel rationeel. Het is een emotioneel 'onderbuik' onderwerp waar door sommige politici gebruik van gemaakt wordt. Terroristen richten zich vooral op het psychologische effect en op zaaien van angst met onvoorspelbaar gruwelijk gedrag. Misschien laten we ons er teveel in meeslepen en vragen we onvoldoende kritisch naar de effectiviteit van allerlei maatregelen. Een belangrijk deel van de verdediging is om ons niet gek te laten maken en ons zo veel mogelijk te concentreren op de feitelijke risico's—zover we die redelijkerwijs kunnen inschatten. Dit deel van de verdediging hebben we zelf in de hand.

Samenlevingen hebben allerlei ongeschreven regels over hoe met elkaar om te gaan en over wat *not done* is. Terroristen houden zich daar weloverwogen niet aan, en raken daarmee een open zenuw. Het blijkt erg moeilijk te zijn daar mee om te gaan, zeker omdat we er collectief sterk op gericht zijn ieder risico uit te bannen en voor alles een schuldige aan te wijzen. Meer controle is dan een begrijpelijke reflex. Maar terroristen blijven, haast per definitie, op zoek naar dat wat zich niet laat controleren[4].

Het is een feit dat westerse overheden hun burgers en bezoekers met meer wantrouwen bejegenen en beter in de gaten zijn gaan houden. Daarbij is het probleem accuut geworden dat er allerlei hiaten zitten in de identiteitsvaststelling, niet alleen bij bezoekers maar ook bij de eigen burgers. In 2005 zijn er in Nederland bijna 200.000 paspoorten als gestolen of vermist opgegeven. Men kan er van uitgaan dat een flink aantal daarvan voor identiteitsfraude gebruikt wordt. Tegen deze achtergrond is bijvoorbeeld het biometrische paspoort ontwikkeld.

Tegelijkertijd zijn de bevoegdheden van opsporingsdiensten vergroot om identificatie te eisen en om informatie op te vragen bij allerlei instanties, zoals bibliotheken of vervoerders. Ook zijn er op Europees niveau inmiddels plannen om de internetproviders en telecommunicatiemaatschappijen te verplichten om de zogenaamde verkeersgegevens van 500 miljoen Europeanen voor anderhalf jaar vast te houden. Het gaat daarbij om gegevens als met wie je wanneer belt (en ook waar, bij mobiele telefoons) of mailt, en waarschijnlijk ook welke webpagina's je bezoekt. Omdat zoektermen voorkomen in de adresbalk betekent dit dat ook alle vragen (en impliciet ook de antwoorden) opgeslagen worden. De opslagtermijn varieert van ergens tussen een half en

[4] Hierbij is ook sprake van een interessante controle-paradox: een zekere overdaad aan regels schept ook vrijheid, namelijk omdat niemand zich meer aan de regels houdt. Het standaard voorbeeld hiervan is Italië: nergens zijn zoveel regels, maar ook zoveel overtreders ervan.

twee jaar. Het moge duidelijk zijn dat hier veel privacygevoelige informatie tussen zit, zoals of ik nu wel of niet regelmatig kijk op de webstek `www.erectieprolemen.nl`. Dat wordt allemaal voor langere tijd vastgelegd, zonder dat ik er controle over heb wie ernaar kijkt, wat ermee gedaan wordt, en waar en wanneer het ooit weer opduikt. De conclusie is gerechtvaardigd dat de overheid haar Big Brother rol nadrukkelijk versterkt en iedereen beter dan voorheen in de gaten houdt. Wat opvalt is dat dit steeds minder selectief gebeurt, maar in de breedte, met sleepnetten (zie het volgend hoofdstuk).

Net als Soft Sister gaat ook de moderne Big Brother pro-actief te werk op basis van de eigen sterke informatiepositie. Uitgaande van de beschikbare gegevens kan de overheid profielen van individuen gaan vormen en daar naar handelen. Je kunt dan (naïef) denken aan een schaal van 1 tot 100 waarop van iedereen aangegeven wordt in hoeverre hij of zij een terrorististisch gevaar oplevert. Op basis van zulke profielen kunnen bijvoorbeeld *black lists* gevormd worden van "vijanden": mensen die buitengesloten moeten worden, bijvoorbeeld uit vliegtuigen of treinen, zie Hoofdstuk 16. Pro-actief handelen is natuurlijk van wezenlijk belang bij terrorismebestrijding omdat alleen reactief opereren geen aanslagen voorkomt. Daarmee is het vooral een zaak van inlichtingendiensten.

Is de individuele privacy hierbij in het geding? We hebben privacy omschreven in termen van het uit elkaar houden van verschillende gegevens die horen bij verschillende rollen van een individu en van de mate waarin een individu ook controle heeft om de bij die rollen behorende informatie gescheiden te houden. De vraag is dus of er bij data vergaring en surveillance door opsporings- en inlichtingen-diensten de controle van individuen afneemt om verschillende rollen uit elkaar te houden. Die controle neemt inderdaad af bijvoorbeeld wanneer aan het licht komt dat een ogenschijnlijk brave apotheker een heimelijke rol speelt als drugshandelaar. Zo'n onthulling zal door niemand aangevochten worden als een onterechte aantasting van de privacy van de apotheker. Maar zelfs wanneer er niets onthuld wordt kan informatie uit verschillende rollen van een persoon in databanken of registers gekoppeld worden buiten de controle van die persoon. Zodra die informatie in zulke databanken zit kan er van alles mee gebeuren—bijvoorbeeld door misbruik of onachtzaamheid, zie Hoofdstuk 16—waar de betrokken individuen geen enkele controle over hebben. Dit kan een zeer verontrustend gevoel van ongepastheid (of zelfs van vernedering) opleveren zeker in de meeste gebruikelijke situaties waarin er geen sprake is van enige vorm van strafbaar gedrag. Hierbij is er dus nadrukkelijk sprake van schending van privacy.

De aantasting van privacy die plaatsvindt bij grootschalige surveillance wordt vooral verdedigd met veiligheidsargumenten. Maar het is belangrijk te beseffen dat het hierbij gaat om 'publieke' veiligheid, in het belang van de samenleving als geheel. Hier liggen gerechtvaardigde belangen, want mogelijk kunnen de verzamelde persoonlijke gegevens gebruikt worden om de schuldigen van een misdrijf veroordeeld te krijgen, of mogelijk zelfs om een terroristische aanslag te voorkomen. De 'persoonlijke' veiligheid wordt echter meestal niet direct vergroot door uitgebreide identificering en monitoring, bijvoorbeeld door het toegenomen risico op identiteitsfraude, misbruik of

gerichte vijandige actie. Hier staat bewust 'meestal niet'. Men zou zich ook kunnen voorstellen dat een gedetailleerd verslag van iemands doen en laten verkregen uit surveillance gebruikt kan worden als verdediging in het geval er sprake is van een valse beschuldiging. Maar ik vermoed dat er toch weinig mensen zijn die zeggen: "sla alles over mij maar op zodat ik zonodig een alibi heb."

Opvallend is dat grootschalige surveillance en opslag, met alle risico's vandien, zich steeds meer richten op de gehele bevolking en niet slechts op de bad guys. Hier moeten de goeden duidelijk lijden onder de slechten. Afgezien van de ethische issues behoeft de resulterende grootschalige privacy aantasting een zeer sterke motivatie op basis van effectiviteit en afweging van risico's. Want nemen we werkelijk zo veel grotere risico's wanneer de overheid zich terughoudend opstelt en surveillance alleen richt op de bad guys en de good guys met rust laat? Misschien vinden we hiermee een redelijke balans tussen publieke en persoonlijke veiligheid. Surveillance, in verschillende gradaties, zou mogelijk ook ingezet kunnen worden als sanctiemiddel. Dit staat ook wel bekend als *revocable privacy*. Tot op zekere hoogte zien we dit al bij het gebruik van elektronische enkelbandjes voor huisarrest. De mogelijkheden zijn echter nog lang niet uitgeput. Na een veroordeling voor fraude zou een s¡traf kunnen zijn dat er grotere identificatieverplichtingen opgelegd worden en dat bijvoorbeeld alle financiële handelingen voor zekere tijd centraal opgeslagen en gecontroleerd worden. Degenen zonder veroordeling (of verdenking) kunnen daar dan van verschoond blijven en er hopelijk vertrouwen in hebben dat zowel veiligheid als privacy bij de overheid in goede handen zijn.

Concluderend kunnen we stellen dat bij de gekozen invulling van de Soft Sister en Big Brother rollen deze broer en zus goede maatjes zijn als het aankomt op pro-actief handelen en het aantasten van de privacy van de burger. Ze doen dat beiden op basis van niet-noodzakelijke tegenstellingen, tussen gemak en privacy enerzijds en tussen veiligheid en privacy anderzijds.

Hoofdstuk 16

Databanken en profilering

De traditionele drager van (gevoelige) informatie is papier, dat relatief gemakkelijk afgeschermd bewaard kan worden in een archief of kluis. Opzoeken en kopiëren van specifieke gegevens kost moeite, en bewaring op de heel lange termijn vraagt om speciale maatregelen om te voorkomen dat de drager gewoonweg vergaat. Moderne informatie is digitaal, nauwelijks gebonden aan een drager, niet zo eenvoudig af te schermen tenzij tezamen met de fysieke drager zoals CD/DVD of memory stick in een kluis. Verder zijn specifieke gegevens eenvoudig te vinden en zonder enige moeite kopieerbaar. Vergankelijkheid van digitale informatie is soms een probleem, maar dan meestal in relatie tot een specifieke informatiedrager—wie heeft nog toegang tot alle bestanden die ooit op eigen floppies zaten—of tot een bepaald formaat voor dataopslag. In dat laatste geval bieden omzettingen tussen formaten echter een uitweg. Gegevens die eenmaal in databanken zitten lijken inderdaad nauwelijks verloren te gaan, zeker wanneer het om waardevolle of gevoelige informatie gaat. Digitale informatie degenereert niet spontaan en wordt alleen verwijderd door, al of niet opzettelijk, wissen of door technische storingen. Digitaal geheugenverlies is daarom zeldzaam in goed georganiseerde omgevingen en persoonlijke controle over eenmaal overgedragen digitale informatie is er niet echt, zie ook Hoofdstuk 12.

De muziek- en film-industrie heeft moeite de juiste, voor hen meest winstgevende, werkwijze te vinden in het tijdperk van digitale informatie. Ook vanuit het perspectief van identiteit en privacy zijn er de nodige uitdagingen. Onwelgevallige foto's of filmpjes zijn niet zomaar van het web te krijgen. Ook is reeds een aantal keer aan de orde gekomen dat steeds meer gegevens over ons en over ons doen en laten in grote databanken terechtkomen. In dit hoofdstuk wordt nader ingegaan op de risico's daarvan voor individuen, met name met betrekking tot profilering.

De Wet Bescherming Persoonsgegevens (Wbp) biedt enige individuele controle over bij anderen opgeslagen gegevens. Men heeft recht op inzage en op aanpassing, of zelfs verwijdering, in geval van fouten. Maar wie maakt hier wel eens gebruik van? Het is meer een principe kwestie dan een praktisch nuttig middel vooral omdat ieder van ons voorkomt in honderden databanken die op ondoorzichtige manier gekoppeld zijn. Je hebt er een dagtaak aan om dat bij te houden en te controleren, zeker wan-

neer die databanken zich ook nog eens in het buitenland bevinden. Dat laatste gebeurt natuurlijk steeds vaker door toenemende outsourcing. Als mensen al bij deze grootschalige opslag stilstaan hoor je snel de verzuchting dat het iets onvermijdelijks is dat kennelijk bij het moderne leven hoort. Individuele lijdzaamheid lijkt inderdaad de best passende houding bij deze centralistische manier van informatie organiseren. Willen we dat; is die lijdzaamheid terecht?

Zijn al die grote, centrale databanken wel zo nodig? Kan het niet wat minder, of wat meer decentraal? En voor wie zijn die databanken zo nodig? Heeft u er zelf baat bij? Zo nee, wie dan wel? In Amerika zijn deze zaken volledig uit de hand gelopen. Wanneer u daar in een hotel verblijft is de kans groot dat bijvoorbeeld uw TV-kijkgedrag geregistreerd wordt en tezamen met uw credit card nummer doorverkocht wordt aan een of andere profielboer. Zulke gegevens worden dan grootschalig verzameld, ook over allerlei andere gedragingen, en verwerkt tot profielen die u als persoon zo goed mogelijk zouden moeten beschrijven. De resulterende virtuele identiteiten worden weer verkocht aan bijvoorbeeld hypotheekverschaffers, verzekeringsmaatschappijen of werkgevers zodat ze 'betere' beslissingen kunnen nemen. Grote bedrijven zoals ChoicePoint en LexisNexis (eigendom van Elsevier) houden zich met dit soort profileringspraktijken bezig. Sinds 9/11 werken deze bedrijven nauw samen met de overheid: commerciële profielen worden daarbij omgevormd tot security profielen.

Voor individuen is er weinig te doen tegen zulk gebruik van bijvoorbeeld TV-kijkgedrag in hotels. De meest effectieve manier om dit soort praktijken tegen te gaan is om helemaal geen identificerende informatie af te staan. Concreet gaat het dan om inchecken in een hotel onder een pseudoniem, of helemaal zonder naam. Een hotel hoeft in principe de naam van de gasten niet te kennen, alleen de kredietwaardigheid. In sommige landen worden wel kopieën van persoonsbewijzen gemaakt die aan de politie overhandigd worden. Elektronisch zou dat kunnen door de hoteleigenaar een versleuteld persoonsbewijs te geven, waarbij voor de versleuteling de publieke sleutel van de politie gebruikt wordt. De hoteleigenaar kan het document dan niet lezen[1].

Voor we nader op deze profilering ingaan is het goed stil te staan bij de risico's van grootschalige gegevensopslag. De beveiliging van databanken tegen inbraak of hacken is verre van eenvoudig en vraagt constante aandacht, zeker wanneer er sprake is van externe toegang, bijvoorbeeld via het internet. Goede beveiling kost alleen maar geld en levert wanneer alles goed geregeld is niks positiefs op. De waarde ervan wordt vooral duidelijk wanneer de dingen niet goed gaan. De gegevens liggen dan echter al op straat en slachtoffers zijn gemaakt. Eenmaal uitgelekte gegevens weer opnieuw beschermen werkt meestal niet. Er zit dan bijvoorbeeld niks anders op dan een nieuw credit card nummer te gaan gebruiken en te accepteren dat de uitgelekte betaalgegevens van het oude nummer openbaar zijn geworden—met allerlei mogelijk resulterende koppelingen tussen rollen. In de Amerikaanse staat Californië bestaat sinds 2003 wetgeving

[1] De hoteleigenaar moet op een of andere manier wel kunnen controleren dat het versleutelde document mijn persoonsbewijs bevat, en bijvoorbeeld niet dat van iemand anders. Daar kunnen slimme cryptografische technieken voor gebruikt worden met zogenaamde *zero knowledge proofs*.

waarbij bedrijven die persoonsgegevens kwijt zijn geraakt, bijvoorbeeld door verlies of diefstal, verplicht zijn de betreffende personen hiervan op de hoogte te brengen. Deze wetgeving is niet alleen gericht op de slachtoffers maar ook op de bedrijven zelf, in de hoop dat alle mogelijke negatieve publiciteit en schadeclaims ze er toe aan zal zetten hun beveiliging te verbeteren.

Wanneer anderen dan betrouwbare bevoegde partijen toegang hebben weten te krijgen kunnen de opgeslagen gegevens misbruikt worden voor identiteitsfraude, of gewoonweg voor reputatieschade. Wanneer hackers de in Europa geplande databanken met verkeersgegevens binnendringen kunnen ze bijvoorbeeld publiceren welke bekende nederlanders bijvoorbeeld wel eens bij een afgelegen relax huis komen—op basis van de locatiegegevens van hun GSM. Soms hoeven er helemaal geen hackers aan te pas te komen en worden door fouten en onbenulligheden van beheerders delen van zulke databanken per ongeluk gelekt, bijvoorbeeld doordat ze op internet verschijnen[2]. Ook kunnen echt kwaadwillenden met toegang gegevens wijzigen, bijvoorbeeld om valse beschuldigingen te kunnen onderbouwen of om levens in gevaar te brengen via medische databanken.

De beheerders van de databanken met gegevens die waardevol zijn voor misbruik zijn kwetsbaar voor geweld of chantage vanuit het criminele of terroristische circuit. Het is een feit dat veel beveiligingsincidenten veroorzaakt worden door *insiders*, net zoals steeds blijkt dat winkelpersoneel voor een flink deel van de winkeldiefstal verantwoordelijk is, en dat politiemensen de politiële informatiesystemen bevragen voor privé-gebruik.

Databanken met gevoelige gegevens kunnen opgezet worden met de beste intenties en met de beste beveiligingsmechanismen omringd. Maar die intenties kunnen natuurlijk veranderen, bijvoorbeeld wanneer een bedrijf in andere handen raakt. Hetzelfde kan gebeuren met overheidsdatabanken wanneer radicaal andere machthebbers het roer overnemen. De Tweede Wereldoorlog vormt daarvoor een voorbeeld. Maar ook wanneer bijvoorbeeld in Nederland twee of drie zware terroristische aanslagen plaatsvinden kiezen we misschien zelf wel een regering die niet alle bevolkingsgroepen even welgezind is. Informatie afstaan aan de overheid betekent impliciet vertrouwen afgeven in alle toekomstige regeringen.

In de begindagen van de automatisering was het voorbehouden aan grote organisaties om er databanken op na te houden met gevoelige persoonsgegevens. Tegenwoordig draait op iedere PC database software die enorme hoeveelheden gegevens aankan, bijvoorbeeld van zelf opgestelde RFID lezers. Deze democratisering van de gegevensopname en verwerking leidt ertoe dat handhaving van regels (zoals uit de Wbp) alleen nog voor de grotere, officiële partijen realiseerbaar is. De bad guys kunnen doen wat ze willen. Daardoor is het des te belangrijker geworden bescherming te richten op het individu—en niet zozeer op centrale databanken—bijvoorbeeld door het gebruik van

[2] In augustus 2006 kwamen per ongeluk 20 miljoen zoektermen van meer dan een half miljoen klanten van de Amerikaanse internet provider AOL op het web te staan, zie bijvoorbeeld `www.aolleak.com`, hetgeen veel onrust veroorzaakte.

domme RFIDs te beperken, zodat kwaadaardige gegevensverzameling minder makkelijk is. Naast de gevaren van bad guys zijn er misschien wel net zo grote gevaren van de goedbedoelende maar naïeve good guys die zelf een databank in elkaar knutselen zonder fatsoenlijk over de risico's of beveiliging na te denken[3].

Van deze lijst risico's dient iedereen zich bewust te zijn die opslag in databanken bepleit—van TV-kijkgedrag en OV- of auto-bewegingen tot en met biometrische data of verkeersgegevens van communicatie. Al die risico's van grootschalige opslag zouden adekwaat afgedekt moeten zijn. Kan dat? Of moeten we beter naar alternatieven kijken?

Opmerkelijk ten slotte is het naïeve vertrouwen dat veel mensen hebben in de gegevens die uit databanken te voorschijn komen: "de computer zegt het dus moet het wel kloppen". Zoals we al in Hoofdstuk 9 gezien hebben leidt attribuutfraude tot veel onbetrouwbare gegevens in databanken. Maar onjuiste invoer, (persoons)verwisseling, beheersfouten of kwaadaardige wijziging zijn ook bekende oorzaken van fouten. De consequenties kunnen zeer onaangenaam zijn. Bekend is het geval van de Amerikaanse senator Ted Kennedy die in 2004 meerdere malen niet aan boord mocht van een binnenlandse vlucht op basis van een persoonsverwisseling met iemand die op de *no-fly* lijst van terroristen stond. Kennedy heeft verschillende keren contact op moeten nemen met toenmalig minister Tom Ridge van *Homeland Security* om de fout hersteld te krijgen. Maar wat moeten u en ik in zo'n situatie? Onlangs bleek bij het inchecken dat er zelfs een 4-jarige kleuter op de *no-fly* lijst stond. Overigens mocht de moeder wel aan boord.

Profilering

In hoofdstuk 5 hebben we gezien dat de verschillende deel-identiteiten die horen bij de onderscheiden rollen in mijn leven door een verzameling attributen gekarakteriseerd kunnen worden. Bij profilering probeert men uit gegevens in databanken zulke attributen te reconstrueren en samen te voegen tot een profiel of virtuele identiteit waarin zo groot mogelijk aantal van mijn rollen combineerd wordt. De impliciete aanname hierbij is dat u en ik, in al onze rollen, dezelfde persoon zijn en blijven. Vanzelfsprekend wordt er geen rekening gehouden met individuele wensen om rollen gescheiden te houden. Dit is een van de onaangename aspecten van profilering. Zo'n profiel wordt vervolgens gebruikt om inschattingen te maken of beslissingen te nemen, zoals hoe een groot risico u vormt bij een hypotheek of verzekering die u af zou willen sluiten, of hoe groot het veiligheidsrisico is bij uw verschijning in de openbare ruimte. Tot op zekere hoogte is zo'n strategie nog wel begrijpelijk. Maar er zijn ook duidelijk risico's en nadelen aan verbonden. Een kwalijke aspect van profilering is bijvoorbeeld dat de criteria die gehanteerd worden zelden expliciet zijn. Misschien zijn ze wel van bedenkelijke aard of kwaliteit. In dat geval kunnen makkelijk onjuiste conclusies getrokken worden. Aanvechting van op profilering gebaseerde beslissingen is moelijk, zeker bij

[3] Bij de Nederlandse *Big Brother Awards* voor privacyschendingen vallen steevast een aantal van dit soort voorbeelden, bij scholen of ziekenhuizen, in de prijzen, zie `www.bigbrotherawards.nl`.

onduidelijke criteria omdat niet herleidbaar hoeft te zijn op welke gronden beslissingen genomen worden. De algemene druk die van profilering uitgaat is om vooral niet op te vallen en je hoofd niet boven het maaiveld uit te steken: je kunt je maar beter conformeren zodat je vooral maar geen *bad profile* krijgt waardoor je op allerlei *black lists* komt te staan en deuren voor je sluiten: *You better be careful, or you will end up on the list!*

Profilering wordt in de commerciële sector graag gebruikt voor gerichte marketing. Dit scheelt kosten en kan potentiële klanten soms verleiden tot onnodige aankopen omdat ze zich persoonlijk aangesproken voelen. Eventuele fouten zijn niet rampzalig. Ik kan er niet van wakker liggen of men mij meent te kunnen karakteriseren als een Amstel of als een Heineken drinker. Toch kan het ook gevoeliger liggen, bijvoorbeeld wanneer de karakterisering wel/niet incontinentie omvat. Maar bij profielen in de beveiligingssector kunnen foute besluiten een veel grotere invloed hebben, zowel bij *false positives* (terrorist mag wel aan boord) als bij *false negatives* (kleuter mag niet aan boord). Ook hier is het een serieus probleem dat de beoordelingscriteria meestal verborgen en misschien wel dubieus zijn. Durft u nog een halal-maaltijd te vragen bij het kopen van een vliegticket naar de Verenigde Staten? Maak je jezelf daarmee verdacht? Waarschijnlijk krijg je een paar bonuspuntjes extra op je persoonlijke terrorisme-spaarkaart. En met welk gedrag krijg je nog meer bonuspunten? Wie beslist dat eigenlijk, en op grond van welke criteria? En hoe raak je zulke bonuspunten ooit weer kwijt, of kan dat überhaupt niet? En wat als iemand zich als jou voordoet en in die hoedanigheid veel punten krijgt? Al deze ongemakkelijke vragen dienen zich aan bij profilering.

Effectiviteit

De prijs van hard disks en geheugenchips daalt al jaren en hun capaciteit neemt nog steeds toe. We kunnen tegen steeds minder kosten steeds meer opslaan. Maar hoe meer er opgeslagen is hoe moeilijker het wordt om iets terug te vinden, of om alle gegevens te transformeren. Hoe groter hoe logger geldt ook voor databanken. Naar verluid heeft Albert Heijn zoveel klantgegevens dat ze zelf niet meer weten hoe ze er effectief gebruik van kunnen maken. Bij de discussies over de Europese regelgeving over opslag van verkeersgegevens (voornamelijk van bellen, emailen en surfen) speelde de gigantische omvang van wat opgeslagen moet gaan worden een voorname rol; providers hebben begrijpelijkerwijs geen zin om voor die opslag (plus beveiliging) op te draaien. Je kunt het vergelijken met de hoeveelheid gegevens die beschikbaar komen wanneer iedere straat in Europa voorzien wordt van camera's. Hebben we er dan nog wel wat aan? Londen hangt al vol met surveillancecamera's, waardoor er ongelooflijk veel beeldmateriaal beschikbaar is. Ik heb me laten vertellen dat de terroristen achter de aanslagen in de zomer van 2005 op beeld gevonden zijn alleen omdat ze toevallig voorkwamen in de eerste partij banden die onderzocht werd. Anders werd er mogelijk nu nog naar ze gezocht.

Ook profilering heeft z'n beperkingen. Stel we hebben een extreem goed veilig-

heidsprofiel met een heel kleine foutmarge van, zeg, één procent. Zo'n foutmarge is volstrekt onrealistisch omdat we helemaal niet weten hoe we terroristen kunnen herkennen. Hoeveel terroristen zijn er eigenlijk? Ook dat weten we natuurlijk niet precies, maar laten het er eens één op de miljoen zijn. Dan moet je dus tienduizend mensen uit een rij van een miljoen halen om die ene (mede) te selecteren. Vervolgens moet je hopen dat je de gezochte terrorist met andere middelen kunt herkennen in de overgebleven groep van tienduizend. Zulke uniforme controlemechanismen zijn voor grote groepen (zoals de gehele bevolking) niet werkbaar. Binnen een reeds geselecteerde kleinere groep zou profilering echter wel nuttig kunnen zijn.

In de commerciële wereld wordt profilering wel vrolijk toegepast op heel grote groepen mensen omdat foute indelingen van individuen daar geen dramatische gevolgen hebben—vooral voor de betrokken bedrijven zelf, natuurlijk.

Gevolgen van surveillance en profilering

In de klassieke natuurkunde hebben observaties geen effect: het maakt voor de loop van een planeet niet uit of je er nu wel of niet naar kijkt. Op het sub-moleculaire niveau worden quantummechanische beschrijvingen gebruikt waarbinnen observaties wel degelijk effect hebben. Voor ons mensen werkt het net zo: voor u en uw partner maakt het waarschijnlijk heel wat uit of u wel of niet geobserveerd wordt wanneer u de liefde wilt bedrijven. Net zo heeft de aanwezigheid van een flitspaal invloed op rijgedrag bij het op oranje springen van een stoplicht.

Surveillance heeft dus een sturende werking, zelfs wanneer je niks te vrezen hebt (zoals bij het vrijen). Op zich is er niks mis met surveillance wanneer de doelen helder bekendgemaakt zijn en breed gedragen worden, zoals bij verkeerscontroles. Voor handhaving van wetten volstaat vaak een vluchtige controle, waarbij er bij goed gedrag geen spoor achtergelaten wordt[4]. De invloed van aan surveillance gekoppelde profilering op gedrag is vaak echter groter: je weet dan vaak helemaal niet waarop geprofileerd wordt en of je wel of niet iets te vrezen hebt. Ook is surveillance voor profilering per definitie niet vluchtig, omdat het er juist om te doen is een spoor vast te leggen en te koppelen aan reeds bestaande informatie voor een profiel.

Het grootschalig gebruik van dit soort profileringsmechanismen voor beveiligingsdoeleinden leidt tot een bange en onzekere bevolking van makke schapen. Aan de angst voor terrorisme wordt de angst voor een *bad profile* toegevoegd. Gaan wij het in de westerse wereld winnen van landen als China en India op het vlak van conformisme en volgzaamheid? Waar liggen onze oorspronkelijke waarden en kracht? Laten we ons zodanig meesleuren en uitdagen door terroristen dat wij over onszelf een veiligheids-communisme afroepen waarbij de belangen van individuen ondergeschikt gemaakt worden aan de vermeende veiligheidsbelangen van het collectief?

[4]Of er ook inderdaad helemaal geen spoor achterblijft is niet altijd duidelijk, bijvoorbeeld bij trajectcontrole.

Hoofdstuk 17

Draagvlak

De overheid draait de laatste jaren met dubbele pet (Big Brother en Soft Sister) de duimschroeven aan: er komen nieuwe identiteiten (BSN) en authenticatiemiddelen (biometrie) waarmee meer identiteitsgebonden informatie vastgelegd wordt en waarmee uitgebreider en strenger gecontroleerd wordt. Vooralsnog lijkt de burger zich van de noodzaak te laten overtuigen door de gehanteerde argumenten veiligheid en gemak. Maar blijft dat zo, zeker op de lange termijn? Wanneer voelen mensen zich teveel als gelabeld vee behandeld en komt er een omslag in het denken en handelen?

De overheid neemt nu al zekere risico's die meestal niet zo expliciet besproken worden. De introductie van het nieuwe paspoort kan gezien worden als een groot sociaal experiment. Zoals bekend bevat het biometrische paspoort een chip die draadloos bevraagd kan worden naar de informatie die erin opgeslagen ligt. Ieder afgegeven paspoort wordt tegenwoordig voorzien van zo'n chip. Maar iemand die zo'n chip echt niet wil kan het paspoort thuis in de magnetron leggen waardoor de chip onklaar gemaakt wordt. Wat overblijft is een traditioneel, nog steeds geldig, paspoort waaruit gegevens alleen op niet-elektronische wijze uitgelezen kunnen worden. De chip is slechts een aanvulling. Indien een of andere actiegroep zich richt tegen het grootschalig gebruik van biometrie en veel mensen ertoe weet aan te zetten om hun eigen paspoortchip onklaar te maken tast dit de effectiviteit van het hele project aan[1]. Er kan immers niet aangetoond worden dat iemand moedwillig de chip in het eigen paspoort opgeblazen heeft. Wanneer tientallen procenten van de Nederlanders met kappotte chips (en onnozele gezichten) aan grensovergangen verschijnen heeft het weinig zin meer de biometrie te controleren.

Een radicalere actiegroep zou een stap verder kunnen gaan en mensen niet alleen vragen om hun eigen paspoortchip onklaar te maken maar zelf ongevraagd chips in paspoorten van anderen gaan vernietigen. Dat zou mogelijk kunnen door af en toe op straat een gedoseerde elektromagnetische puls uit te stralen waardoor chips in paspoorten in de directe omgeving het begeven. Hierbij loopt men wel het risico dat veel meer apparatuur vernield wordt, zoals bankpassen, organisers, GSMs, of zelfs pacemakers.

[1]Denk bijvoorbeeld aan de impact van `www.wijvertrouwenstemcomputersniet.nl`.

In het eerste geval van zelfgekozen vernietiging kan de overheid nog enige invloed uitoefenen door het mensen die met een kappotte paspoortchip de grens passeren zodanig onaangenaam te maken (ophouden of visiteren) dat men zou willen dat de chip werkte. Maar het is de vraag of men individuen verantwoordelijk kan houden voor het correct functioneren van hun paspoortchip. In het tweede geval van ongevraagde vernietiging kan niet veel anders gedaan worden dan de bronnen van de elektromagnetische pulsen proberen op te sporen.

Ook kan de overheid bij dit soort ondermijning besluiten een tandje hoger te schakelen en de biometrische gegevens van burgers niet meer op de paspoorten op te slaan maar enkel nog in een centrale databank—met alle risico's vandien voor de burgers, zie Hoofdstuk 13. Bij verificatie wordt de afgegeven vingerafdruk dan vergeleken met de versie in de databank. Bij identificatie wordt een afgegeven vingerafdruk opgezocht in de databank om de bijbehorende identiteit te vinden.

Maar ook bij zo'n centrale databank kunnen onwillige en dwarse burgers roet in het eten gooien. Stel dat veel mensen uit protest zelf hun vingerafdrukken op het web plaatsen. Dit geeft anderen de mogelijkheid zomaar een vingerafdruk te kiezen, te downloaden, op een vliesje na te maken, en te misbruiken. Mocht mijn vingerafdruk dan ergens op een plaats van een delict aangetroffen worden kan ik altijd roepen: "hé, mijn vingers staan op het web; dit kan iedereen geweest zijn". Deze vorm van ondermijning heeft natuurlijk alleen zin wanneer niet alleen mijn vingerafdrukken maar ook die van veel anderen op het web staan. Zo'n vlucht vooruit ondermijnt de identificatiemogelijkheden van centraal opgeslagen biometrie.

Het onderliggende punt is: *don't push things too far*. De overheid is uiteindelijk afhankelijk van draagvlak onder de bevolking. Maar niet alleen dat. Door een toenemend leunen op technische maatregelen maakt de overheid zich ook kwetsbaarder voor de waarschijnlijk kleine groep van technisch onderlegde individuen die het systeem kunnen misbruiken of zelfs saboteren. Techniek maakt kwetsbaar, zeker wanneer de inzet een centralistisch karakter heeft.

Maar onwillige burgers vormen niet alleen een gevaar in destructieve zin. Ze kunnen ook op eigen wijze creatief gebruik maken van de technische mogelijkheden waarbij de overheid het nakijken heeft. Een voorbeeld is de 'cryptophone', een commercieel verkrijgbare niet-afluisterbare mobiele telefoon. Ook blijkt dat het aftappen van telefoongesprekken steeds minder effectief wordt omdat criminelen (of andere burgers) op alternatieve wijze gaan communiceren, zoals bijvoorbeeld via chatkanalen in multi-player online games. Moet dat ook allemaal opgeslagen en afgeluisterd worden?

Soms zijn naïeve oproepen hoorbaar die stellen dat heel het internet (of alle PCs) onder strakke controle geplaatst zouden moeten worden en dat alle online activiteiten strenge authenticatie zouden moeten vereisen zodat tenminste duidelijk is wie wat uitvreet. Afgezien van de technische en organisatorische complexiteit van zo'n omschakeling is het belangrijk te beseffen dat dergelijke vergaande maatregelen online niet mogelijk zijn zonder vergelijkbare draconische en dictatoriale maatregelen offline, in het dagelijkse leven. Vrijgevochten burgers die geen behoefte hebben aan dergelijke betutteling en controle zouden immers hun eigen parallelle internet kunnen gaan opzetten, bijvoorbeeld via aan elkaar geknoopte locale draadloze netwerken[2]. De techniek en de vertrouwdheid met het gebruik ervan zijn inmiddels zodanig verspreid in onze samenleving dat alleen Noord-Koreaanse omgangsvormen tussen staat en burgers dergelijke iniatieven zouden kunnen onderdrukken. *Don't push things too far*.

Technische kennis is tegenwoordige wijd verspreid in de samenleving. Dit vormt de basis voor innovatie en economische kracht. Tegelijkertijd betekent deze verspreiding dat de overheid geen technische monopolies heeft en kan gebruiken voor de eigen Big Brother en Soft Sister rollen. Afgezien van de morele argumenten zijn er dus voldoende pragmatische redenen waarom de nodige terughoudendheid in overheidsmaatregelen gepast is: technisch onderlegde enkelingen kunnen het systeem ondermijnen. In dit stadium is de machtsbalans tussen burgers en overheid gelukkig nog niet volledig omgeslagen in de richting van de overheid.

Indien hardware (apparatuur) en software (programma's) goedkoop en breed verkrijgbaar zijn kunnen we die mate van verspreiding misschien maar beter accepteren en benutten in een meer gedecentraliseerde identiteitsinfrastructuur.

[2] Zie bijvoorbeeld het initatief `www.fon.com`.

Hoofdstuk 18

Informatie en macht

Een oude uitdrukking zegt: kennis is macht. Wanneer u veel over mij weet kunt u mij bijvoorbeeld chanteren; iets onschuldiger kunt u ook anticiperen op mijn handelingen en daar ten eigen bate op inspelen. Eigenaren of beheerders van grote databanken met persoonsgegevens hebben een sterke informatiepositie en daarmee macht over de betrokkenen. Een medewerker van een credit card maatschappij kan u of mij mogelijk chanteren op basis van uitgaven in bepaalde etablissementen van plezier.

Macht heeft de neiging zichzelf te versterken. Een eenmaal opgebouwde positie wordt zelden spontaan opgegeven. Regulering is vaak de enige manier om degenen aan de zwakke kant van de machtsverhouding te beschermen. Kenmerkend voor een rechtstaat is een redelijke verdeling van macht.

Digitale technieken kunnen door verschillende partijen in het machtsspectrum gebruikt worden. In de huidige 'platte' wereld kunnen individuen er hun invloed mee vergroten, bijvoorbeeld door via blogs zelf hun 'boodschap' te verspreiden, hun talenten of diensten wereldwijd aan te bieden, of verkopers te dwingen tot een gunstig prijsniveau via uitgebreide online prijsvergelijking. Ook kunnen dissidenten bijvoorbeeld via versleuteling vertrouwelijk en anoniem communiceren en zich daarmee onafhankelijk organiseren. Maar het lijkt erop dat vooral de traditionele machthebbers van de nieuwe technieken profiteren en er hun machtpositie mee versterken. Vaak zijn zij het immers die beslissen over de organisatie of architectuur van de beschikbare techniek, zoals over het wel of niet centraal opslaan van vervoersbewegingen bij rekeningrijden (zie Hoofdstuk 3). Op eenzelfde manier willen de grote partijen achter de OV-chipkaart zoveel mogelijk informatie over de reizigers identificeerbaar opslaan omdat zulke informatie macht en geld oplevert. Alleen regulering, opgelegd door de overheid of het College Bescherming Persoonsgegevens (CBP), dwingt deze partijen tot enige matiging. Binnen discussies over structurele keuzes bij informatisering speelt altijd een machtsvraag, namelijk wie er zeggenschap krijgt over welke informatie—en dus over de bijbehorende macht.

De overheid heeft hierbij een speciale positie. Het naïeve beeld is dat weinig regulering goed is voor de vrijheid van de burger: hoe minder de overheid zich met zaken bemoeit hoe vrijer de burger is om zelf te handelen. In een meer genaunceerd beeld

garandeert overheidsregulering juist de individuele vrijheid. De huidige samenleving is zo complex dat regels juist nodig zijn om zodanige omgangsvormen mogelijk te maken dat individuen vrij kunnen handelen. Die regels moeten met name de machtige partijen—inclusief de overheid zelf—beperken in de invloed die ze over zwakkere partijen kunnen uitoefenen. De paradoxaal klinkende situatie dat vrijheid geregeld moet worden vraagt om politiek waarin betuttelende socialisten en vrijzinnige liberalen tot een overstijgende synthese komen.

Vanuit dit perspectief is een actief overheidsbeleid noodzakelijker dan ooit bij de grote maatschappelijke informatiseringsprojecten die nu in gang gezet zijn of worden, zoals het biometrische paspoort, de OV-chipkaart, en digitale informatievoorziening en transacties. Indien we op dit gebied enige bescherming van het individu wensen, bijvoorbeeld in het systematisch gebruik van pseudoniemen en andere Privacy Enhancing Technologies (PETs), zal dit afgedwongen moeten worden via integere overheidsregulering. De betrokken 'machtige' partijen die de keuzes maken zijn uit zichzelf niet geneigd kleinschaligheid en belangen van individuen voorop te stellen.

Het is hierbij de moeite waard het pleidooi te herhalen dat opgeschreven is in het Actieprogramma 'Andere Overheid' (2003): "Meer zeggenschap, meer mogelijkheid voor eigen initiatieven, meer betrokkenheid bij politiek en bestuur en meer gelijkwaardige verhoudingen tussen burgers en overheid." Met name deze gewenste gelijkwaardige verhoudingen vereisen een actieve stimulering van decentrale opslag van gegevens en van individueel zeggenschap en beheer over de eigen persoonsgegevens. De fundamentele vraag is of de overheid deze fraaie intenties werkelijk meent en ook waar wil maken door distributie van gegevens en daarbijhorende macht. Zal onze door terrorisme geobsedeerde overheid in staat zijn om haar burgers die macht in handen te geven? Het gaat dan niet om zoiets onbenulligs als een Persoonlijke Internet Pagina[1] bij de overheid waarop verschillende gegevens en procedures bekeken en gevolgd kunnen worden, maar om een zodanig individueel zeggenschap dat de overheid zelf ook niet meer bij de gegevens kan—tenzij de burger daar zelf toestemming voor geeft, of de overheid speciale gerechtelijke volmachten heeft. Ik meen werkelijk dat zo'n verdeling van macht via technische middelen noodzakelijk is om op de langere termijn de fundamentele waarden van individuele autonomie die ten grondslag liggen aan onze samenleving overeind te kunnen houden.

Good guys en bad guys

De toegenomen technische mogelijkheden geven de overheid natuurlijk verleidelijk veel mogelijkheden. Vroeger waren de surveillancecapaciteiten beperkt en werden alleen diegenen in de gaten gehouden die eerst als verdachten gekenmerkt werden. Dat laatste gebeurde, in juridische termen, op basis van een redelijk vermoeden. Tegenwoordig kan iedereen in de gaten gehouden worden en hoeft surveillance niet meer om praktische redenen beperkt te worden tot verdachten. Die mogelijkheden worden dan

[1] Ofwel PIP, zie `www.e-overheid.nl/sites/pip/`.

ook graag benut, bijvoorbeeld in de afgedwongen opslag van verkeersgegevens van alle Europeanen.

In der Beschränkung zeigt sich der Meister. Ondanks deze verleidelijke mogelijkheden is het misschien toch gepast deze surveillance welbewust te beperken tot de bad guys en de overgrote meerderheid van good guys weloverwogen met rust te laten, onder het motto *select before you collect*. Sterker nog, surveillance kan als sanctiemiddel selectief ingezet worden—onder de noemer *revocable privacy*—waarbij bijvoorbeeld van veroordeelde pedofielen of bezitters van kinderporno het internetverkeer voor langere tijd wel opgeslagen wordt. Deze strategie sluit aan bij fundamentele principes: net zoals niemand schuldig is tenzij dat bewezen is getuigt het van beschaving om niemand aan surveillance te onderwerpen tenzij daar gegronde redenen voor zijn. Is men eenmaal een bad guy dan kan surveillance in meer of minder mate ingezet worden als straf. Wat doe je liever: een jaar zitten of tien jaar rondlopen waarbij je locatie continu geregistreerd wordt?

Deze strategie gaat uit van een tweedeling in good guys—die niet geobserveerd hoeven te worden—en bad guys—die daaraan wel in bepaalde mate onderworpen worden. Een fundamenteel punt van zorg bij deze strategie is hoe we deze opdeling in good en bad guys dan moeten bepalen. Juist daarvoor lijkt grootschalige surveillance immers nodig. Vaak weten we vooraf niet wie de bad guys zijn, en kunnen we dus maar beter iedereen in de gaten houden zodat we uit de resulterende gegevens informatie kunnen halen over degenen die achteraf 'bad' bleken te zijn.

Dit is een valide redenering, waarop ik twee tegenargumenten heb. Om te beginnen blijkt dit selectie-issue in de praktijk niet zo'n probleem te zijn, zelfs niet in de terrorismebestrijding. Van alle publiekelijk bekende gevallen van terrorisme waren de daders vooraf reeds in beeld bij de inlichtingendiensten. Ze waren al bekend als potentieel 'bad', wat voldoende reden zou moeten zijn om uitgebreidere surveillancemechanismen in te schakelen. De inlichtendiensten hebben in deze gevallen vaak ook adekwaat gehandeld, maar niet altijd (zoals bij de moord op van Gogh). Meestal is het probleem in die kringen dat er juist teveel informatie voorhanden is en dat de uitdaging erin zit om de ruis eruit te filteren om de echte dreigingen over te houden[2].

De bad guys zijn dus meestal wel bekend. Maar toch zijn er situaties denkbaar waarbij een good guy die niet onder surveillance staat plotseling bad wordt waardoor er geen of weinig achtergrondgegevens beschikbaar zijn voor vervolging en veroordeling. Dit is inderdaad een risico. Voor een goede afweging van dit risico, en voor een goede verdere discussie over de afweging 'alleen gerichte' of 'juist ongerichte' data surveillance, is het noodzakelijk dat er een beter inzicht komt in de grootte ervan. Dit vergt nader onderzoek, liefst door een onafhankelijke commissie met toegang tot vertrouwelijke gegevens. Het gaat hier immers om fundamentele vragen. Ik ben vooralsnog sterk geneigd te denken dat we het hier hebben over een risico dat we moeten

[2] Meer onafhankelijke studie naar de effectiviteit van verschillende methoden van terrorismebestrijding is dus dringend gewenst. Elementen daarvan zijn te vinden in: Rob de Wijk en Carla van Relk, *Doelwit Europa: Complotten en aanslagen van moslimextremisten* (Mets & Schilt, Amsterdam, 2006), ook al zijn detectiemethoden daar niet zelf onderwerp van studie.

nemen wanneer we niet in een politiestaat terecht willen komen. Dit is mijn tweede punt. Deze bereidheid dit risico omwille van de beschaafdheid van onze samenleving te accepteren zal echter vooral onder druk komen te staan bij plotselinge ernstige misdrijven of aanslagen wanneer de bevolking geschokt is en er incident-politiek bedreven wordt. Echter ook in dat soort omstandigheden is het belangrijk de rug recht te houden en uit te stralen: wij houden vast aan onze waarden en kunnen dit aan. Bedreigende en gewelddadige politieke bewegingen komen op en verdwijnen ook weer. Repressieve infrastructuur verdwijnt minder snel.

Deel V

Hoe verder?

Hoofdstuk 19

Hoeveel moeite willen we doen?

De beschouwingen in de voorafgaande hoofdstukken bevatten een rode draad waarin persoonlijke autonomie verdedigd wordt in tijden waarin individuen onder druk staan van overheid en bedrijfsleven om vooral transparant, voorspelbaar en conformistisch te leven omwille van organisatorische en commerciële belangen. Privacy speelt daarbij een belangrijke rol in de vorm van zeggenschap over de eigen rollen en over de daarbij horende deel-identiteiten en gegevens. Onderdeel van die rode lijn is wantrouwen tegenover een centralistische ICT-organisatie waarbij individuen steeds indringender door computers omringd worden en aan alle kanten bevraagd en besnuffeld worden door apparaten die zij gedwongen worden te vertrouwen zonder dat ze daar adekwate middelen voor in handen hebben. Daartegenover wordt hier gepleit voor ICT met een menselijke maat waarbij een aanzienlijke mate van individuele autonomie over de eigen rollen en de daarbij behorende gegevens zou kunnen (blijven) bestaan.

In dit laatste deel van het boek zal de blik meer op de toekomst gericht worden. In dit eerste hoofdstuk zullen op basis van het voorafgaande twee mogelijke toekomstscenario's (als uitersten) geschets en besproken worden.

1. In het eerste scenario hebben Big Brother en Soft Sister de handen stevig ineengeslagen: burgers hebben een chip in de nek en lopen voortdurend door (al of niet zichtbare) controlepoortjes waar hun identiteit gecontroleerd en geregistreerd wordt. Bij ieder loket, dienst, of informatiezuil worden mensen automatisch herkend, en op hun wenken bediend, uitgaande van beschikbare profielen. Deze profielen (of virtuele identiteiten) worden voortdurend aangepast op basis van het geregistreerde gedrag, zodat de dienstverlening steeds optimaal aansluit bij eerdere wensen. Hiervoor is het toegestaan dat iedereen gegevens en profielen over anderen opslaat en bewerkt, binnen algemene kaders. Afwijkingen van geoorloofd gedrag worden direct opgemerkt, en leiden onmiddelijk tot beperking van autorisaties, zodat de mogelijkheid tot voortzetting of uitbreiding van het vertoonde ongewenste gedrag gelimiteerd is. Het vaststellen van deze afwijkingen en het opleggen van deze beperkingen van eigen diensten is ook aan iedereen toegestaan.

2. In het tweede scenario hebben mensen zelf controle, niet alleen over hun eigen (persoons)gegevens en nagelaten digitale sporen, maar ook over de momenten en manieren waarop ze zich authenticeren. Daarbij zijn ze in staat eerst de aard en authenticiteit vast te stellen van het controlepunt: de omgeving authenticeert zich eerst. Bij een loket / dienst / informatiezuil kiest de burger zelf welke informatie op dat moment beschikbaar wordt gesteld (ook over de eigen identiteit) en onder welke gebruiksvoorwaarden. Deze privacy is echter individueel (en niet collectief) *revocable*: bij gerechtvaardige verdenking of na veroordeling kan additionele registratie van gedrag opgelegd worden.

De grote vraag is nu: waar kiezen we voor?

Het eerste scenario biedt veiligheid en gemak, ervan uitgaande dat alles werkt zoals het bedoeld is en misbruik van het systeem uitgesloten is zodat individuele vrijheid (binnen de door het systeem vastgestelde grenzen) gegarandeerd is. Deze symbiotische structuur van in een groter geheel geïntegreerde individuen heeft echter totalitaire trekjes die een zeker gevoel van ongemak oproepen. Moeten we maar leren omgaan met dit gevoel van ongemak? Is dit iets waar we vanzelf wel aan wennen en waar we ons op een gegeven moment niet meer van bewust zijn—net zoals slechts weinigen er moeite mee hebben dat ze voortdurend via hun mobiele telefoon traceerbaar zijn.

Het tweede scenario heeft niet deze ingebouwde symbiose maar kent een duidelijker scheiding tussen individuen en hun omgeving. Dit vraagt echter een veel grotere inzet van individuele mensen. Daarnaast vraagt het ook (meestal) om extra moeite bij de inrichting van ICT-systemen om de geschetste decentrale controle mogelijk te maken. Hebben we daar de extra moeite en kosten voor over?

Zoals eerder genoemd vraagt individuele vrijheid om een actieve opstelling om zelf keuzes te maken en je niet te laten leiden en verleiden door interne impulsen en externe verlokkingen. Niet iedereen is daar in gelijke mate toe geneigd (of in staat). Op een vergelijkbare manier vraagt (informationele) autonomie om een actieve opstelling. De Franse filosoof Foucault riep: maak van je leven een kunstwerk! Zoiets lijkt ook in deze context van toepassing. Wie wil (of kan) dat?

De grote vraag is dus: wat hebben we er voor over? Ikzelf ben wel principieel in dit soort zaken, maar ik ben ook vaak lui en gemakzuchtig. Ook al ligt mijn sympathie nadrukkelijk bij het tweede scenario, ik realiseer mij terdege dat ik daar wel heel wat voor moet doen. En ik niet alleen.

Is het tweede scenario wel realistisch? Misschien niet. Misschien moeten we over enige tijd mistroostig (*sadder but wiser*) constateren dat idealen als privacy en individuele autonomie te hoog gegrepen zijn voor de mensheid en dat (onze manier van inzetten van) ICT tot panoptische controlerende structuren leidt en het in die zin van ons over neemt. Historisch gezien hebben die privacy en autonomie dan maar relatief korte tijd bestaan. Mogelijk zijn het toch geen wezenlijk menselijke trekken.

Voor het ooit zover komt, wil ik, misschien tegen beter weten in, nader onderzoeken hoe die individuele autonomie met moderne ICT wel ondersteund zou kunnen worden. Mogelijk is daarmee het tweede scenario te realiseren, of toch ook een redelijke mengvorm van de als twee uitersten bedoelde scenario's. Daar zal de rest van dit laatste deel van het boek aan gewijd zijn.

Hoofdstuk 20

Richtlijnen

Het tweede “autonomie” scenario uit het vorige hoofdstuk zal hier nader uitgewerkt in een aantal algemene richtlijnen voor het gebruik van ICT in onze samenleving. Daarbij worden veel aspecten open gelaten over hoe die richtlijnen het beste in de praktijk gebracht zouden kunnen worden. In het volgende en laatste hoofdstuk wordt daar wel een mogelijke, meer concrete technische invulling aan gegeven in de vorm van een persoonlijke apparaatje dat individuen helpt bij het eigen beheer van identiteiten, gegevens en policies.

1. Decentraliseer gegevensbeheer

In de Europese politiek geldt het zogenaamde subsidiariteitsbeginsel. Het is erop gericht besluitvorming zo dicht mogelijk bij de burger te laten plaatsvinden en alleen naar een hoger centraal niveau te tillen—en dan nog in beperkte mate—indien daar een aantoonbare noodzaak voor aanwezig is. Eenzelfde principe zou moeten gelden voor gegevensbeheer: laat gegevens zo dicht mogelijk bij de mensen zelf en centraliseer alleen wanneer daar een dwingende inherente noodzaak voor aanwezig is.

De achterliggende gedachte is dat ik zeggenschap zou moeten hebben over gegevens over mij. Indien iemand anders ze nodig meent te hebben moet er netjes om gevraagd worden. Grote onpersoonlijke databanken met persoonlijke gegevens werken vervreemdend en kennen veel bedrijfsrisico’s voor de betrokkenen die kunnen leiden tot compromitering of identiteitsfraude. Decentraal beheer benadrukt de eigen verantwoordelijkheid van de burger en geeft mogelijkheden om zelf te kiezen hoe het beste met de gegevens om te gaan. Misschien kiezen sommigen er dan zelf wel voor om het beheer van de eigen gegevens uit handen te geven aan vertrouwde grote partijen. Maar anderen beheren de eigen gegevens mogelijk liever zelf.

2. *Select before you collect*

Het is ongepast en onwenselijk wanneer de overheid van alle burgers informatie verzamelt ‘voor het geval dat’ (*collect before select*). Ondanks mogelijk enige effectivi-

teitsvoordelen bij de opsporing en vaststelling van strafbare feiten moeten we zoiets niet willen. Deze aanpak verstoort de machtsbalans tussen overheid en burgers, en leidt, zeker in combinatie met uitgebreide profilering, tot gedweeë, conformistische en bange onderdanen.

In plaats daarvan moeten we, ook nu de technische mogelijkheden voor grootschalige surveillance beschikbaar zijn, er expliciet voor kiezen die niet in te zetten en de grote meerderheid nadrukkelijk met rust laten. Hiermee toont de overheid vertrouwen in en respect voor de eigen burgers, maar niet noodzakelijkerwijs naïviteit. De bad guys moeten wel degelijk in de gaten gehouden worden, maar alleen na selectie. Informatie kan ook al in een vroeg stadium verzameld worden, op basis van een redelijk vermoeden dat onafhankelijk getoetst wordt. Indien iemand eenmaal terecht verdachte is mag wat mij betreft de volledige staatsmacht ingezet worden. Maar het zou een kenmerk moeten zijn van een geciviliseerde samenleving om, ondanks de beschikbare technologische mogelijkheden, toch af te zien van de inzet van die staatsmacht (bijvoorbeeld via uitgebreide data surveillance) zonder selectie vooraf. Dit is een grote uitdaging omdat het gaat om een fundamentele beperking van de macht van de overheid.

Bij de Europese regelgeving met betrekking tot opslag van verkeersgegevens wordt deze richtlijn geschonden. Die moet dan ook snel van tafel.

3. Surveillance als straf

Intensieve surveillance van het dagelijkse leven is dermate onprettig dat het ook goed ingezet kan worden als straf volgend op een veroordeling. Dit sluit aan bij reeds bestaande praktijken waarbij een vorm van huisarrest opgelegd kan worden die gecontroleerd wordt via een zendertje in een enkelband bij de veroordeelde. De kern van de straf is een vermindering van anonimiteit tegenover bevoegde instanties gekoppeld aan gedwongen centrale vastlegging van bijvoorbeeld alle communicatie, locatie en transactie gegevens. Net als medische zorg steeds persoonlijker bij mensen thuis plaatsvindt kan bestraffing op deze wijze ook gerichter (en mogelijk ook goedkoper) in de eigen omgeving plaatsvinden. Zulke gedwongen surveillancemaatregelen hebben zowel een vergeldende als een preventieve werking: de veroordeelde wordt tegelijkertijd geconfronteerd met onaangename consequenties en met een panoptische blik die iedere mogelijke volgende misstap direct registreert—en liefst ook een passende reactie direct in gang zet.

Net als in het vorige punt gaat het hier om een selectieve, beperkte inzet van surveillance, en niet om een collectieve, onbeperkte vorm die de gehele bevolking raakt. Ook dit vergt een bewuste keuze: de gewone burger krijgt het vertrouwen en de middelen om de eigen identiteit en gegevens te beschermen, *tenzij*.

4. Attributen in plaats van identiteiten

Opvallend veel transacties kunnen plaatsvinden op basis van attributen en hoeven niet te beschikken over de identiteiten van de betrokkenen, zie Hoofdstuk 11. We moeten ons beter gaan realiseren dat overal je naam (of andere identificerende gegevens) achterlaten je kwetsbaar maakt voor identiteitsfraude en ongebreidelde profilering. Waarom staat er bijvoorbeeld eigenlijk een naam op een bankpasje? Waarom niet alleen een nummer, of een pseudoniem—en dan liefst nog een steeds wisselend eenmalig pseudoniem zodat kwaadaardig hergebruik niet mogelijk is? Of waarom gebruiken we geen anoniem elektronisch geld, in plaats van de huidige chipknips waarmee betalingen traceerbaar zijn? Een winkelier hoeft toch niet meer van mij te weten dan dat ik voldoende kapitaalkrachtig ben voor de geplande aankoop. Technisch zijn zulke identiteitsarme transacties inmiddels allemaal mogelijk. We kunnen computers gebruiken om de bijbehorende administratieve details (zoals tijdelijke identiteiten) bij te houden en af te handelen zodat er geen overlast is voor de gebruikers. Degenen echter die beslissen over de ICT-infrastructuur zijn tot nu toe niet of nauwelijks bereid geweest—of ertoe gedwongen—zulke privacyvriendelijke mechanismen te implementeren. Maar misschien ook is het inzicht in de risico's voor ons als individuen op de lange termijn onvoldoende aanwezig, en zijn er nog te weinig dingen goed fout gegaan. Een groot deel van de aantasting van onze privacy door identiteitsrijke technieken verloopt sluipenderwijs. Misschien is er eerst een dramatische gebeurtenis nodig—zoals een moordaanslag op een bekende Nederlander met een bom die getriggerd wordt door een RFID chip van het slachtoffer—voordat we meer geneigd raken identiteiten af te schermen.

5. Laat de omgeving zich eerst authenticeren

De combinatie van toegenomen automatisering en nadruk op veiligheid leidt ertoe dat ik mij steeds vaker moet identificeren en authenticeren, bijvoorbeeld bij binnenkomst van landen of gebouwen en bij allerlei dagelijkse handelingen zoals elektronische betalingen. Bij al die authenticaties geef ik gevoelige informatie over mijzelf prijs, zoals PINs, wachtwoorden, paspoortgegevens of vingerafdrukken. Al die gegevens kunnen misbruikt worden voor identiteitsfraude. Het is dus van wezenlijk belang dat ik deze gegevens alleen aan betrouwbare partijen afgeef. Wanneer je mensen steeds weer door controlepoortjes wil jagen is het wel *fair* om ze ook de mogelijkheid te geven om vooraf vast te stellen of ze wel door een 'echt' poortje lopen en niet door een 'nep' poortje van een of andere criminele organisatie die uit is op identiteitsroof.

Maar hoe weet ik eigenlijk of ik met de juiste, betrouwbare tegenpartij te doen heb? Dat weet ik alleen wanneer de andere partij zich eerst geïdentificeerd en geauthenticeerd heeft. Dit is dus een fundamentele vereiste. Geef niks van jezelf weg voordat je zeker weet met wie je toe doen hebt en of die partij betrouwbaar is en verantwoordelijk gehouden kan worden voor eventueel misbruik.

In intuïtieve zin kennen we dit principe, ook al gaan we er vaak slordig mee om.

Wie let er expliciet op of een geldautomaat wel echt is? Dit is een serieuze kwestie omdat we de automaat zowel onze pas als PIN geven, en daarmee volledige toegang tot onze bankrekening. Een probleem is dat we eigenlijk niet zoveel middelen in handen hebben om de echtheid van zo'n automaat vast te stellen. Meestal geeft de locatie bij een bankgebouw of postkantoor enig vertrouwen. Maar zou u ook uw pas en PIN geven aan een geldautomaat op de autosloop?

Wanneer het gaat om communicatie tussen computers kunnen en moeten we dit soort zaken wel goed regelen. Onderdeel van deze richtlijn is dat een RFID-chip die ik (gedwongen) bij me draag nooit zomaar het eigen nummer uit mag stralen, maar eerst moet controleren wie de vragende partij is. Dit vereist technisch ingewikkelder chips dan op dit moment gebruikt worden. Maar het voorkomt wel dat kwaadaardige handelingen tegen mij uitgevoerd kunnen worden alleen omdat ik herkend wordt via een RFID-chip. Deze richtlijn is in het belang van mijn persoonlijke veiligheid.

Toch staat deze richtlijn de openbare veiligheid niet in de weg. Ik heb er geen moeite mee wanneer op cruciale momenten—zoals bij grenspassage of binnenkomst van een beveiligd gebouw—mijn identiteit automatisch en elektronisch gecontroleerd wordt, zolang mijn persoonlijke computer (zie het volgende Hoofdstuk) maar kan herkennen dat het een authentiek verzoek is dat (elektronisch) ondertekend is door de bevoegde autoriteiten.

6. Hang een vangnet

In de (commerciële) ICT-sector bestaat vaak een groot vertrouwen in de mogelijkheden en in het functioneren van computersystemen. In de praktijk weten we inmiddels dat er ook vaak van alles fout gaat, bijvoorbeeld doordat de beveiliging niet in orde is of doordat mensen bewust of onbewust fouten maken bij de invoer van gegevens of bij het gebruik van het systeem. Daardoor kunnen (automatisch) beslissingen genomen worden die nadrukkelijk onbedoeld zijn maar niet altijd direct als zodanig herkend worden.

Het is dus belangrijk hier in het ontwerp van systemen al rekening mee te houden door te zorgen voor een vangnet voor *fallback* procedures[1]. Waar moet iemand heen van wie de DigiD misbruikt is, of die bij hoog en bij laag beweert een ander te zijn ondanks biometrische identificatie, of die zweert wel de houder van een paspoort te zijn terwijl de biometrische verificatie faalt? Het is erg verleidelijk om als ontwerper zo'n situatie af te doen als: dat kan echt niet! Maar in de praktijk blijken er altijd zaken anders te kunnen lopen dan voorzien. Er moet ruimte zijn om daar mee om te gaan, om betrokkenen zich niet verloren en vervreemd te laten voelen en om draagvlak te houden. Negatieve ervaringen verspreiden zich verrassend snel, en niet altijd op even waarheidsgetrouwe wijze.

Vooral voor de overheid is het van belang om niet geassocieerd te worden met

[1] Hierbij moet er voor gezord worden dat de fallback procedures zwaarder zijn dan het primaire proces, vooral om dat primaire proces niet te ondermijnen.

het vervreemdende effect van slecht functionerende informatietechnologie—enigszins vergelijkbaar met het vervreemdende effect van bureaucratie.

7. Dump geen risico's

Het is verleidelijk de risico's van het gebruik van computersystemen bij de zwakkste partijen te leggen. Vaak zijn dat de gebruikers zoals u en ik. Het werkt echter veel beter om de risico's en de lasten daarvan te leggen bij de partijen de er ook het meeste aan kunnen doen. Soms moet zoiets expliciet afgedwongen worden via regelgeving of afspraken. Dat biedt de beste garantie dat risico's onder controle blijven.

8. Laat je niet gek maken

Hopelijk spreekt deze richtlijn voor zich. De dreiging van terroristische aanslagen is serieus en angstaanjagend. Maar dat is geen reden om niet kritisch te kijken naar effectiviteit en neven-effecten van allerlei maatregelen. Politici kunnen in het licht van de dreigingen niet niets doen, en doen dus soms maar snel wat. Het gaat daarbij om ingrijpende aangelegenheden die de fundamenten van onze samenleving raken. Het is dan niet gepast om beslissingen impulsief te nemen, als directe reactie op incidenten. De laatste jaren hebben we gezien dat vervolgmaatregelen soms al vastgesteld worden voordat de daaraan voorafgaande maatregel goed en wel van kracht is (denk aan opslag verkeersgegevens na het bevriezingsbevel voor telecommunicatiegegevens[2]) of geëvalueerd is (centrale opslag biometrie na de identificatieplicht).

Het is belangrijk adekwaat te reageren op dreigingen. Maar het is ook goed je te realiseren dat het opleggen van zware veiligheidsmaatregelen maar beperkte waarde heeft—terroristen zoeken toch altijd de zwakste schakel—en ook nieuwe risico's introduceert voor degenen die overal hun identiteit en gegevens moeten achterlaten. Het is daarentegen helemaal niet zo'n onredelijke strategie om je kwetsbaarheid te tonen en uit te buiten. Nederlandse militairen staan in Irak en Afghanistan bekend om deze *Dutch approach*, waarbij laagdrempelig contact wordt onderhouden met de locale bevolking en men expliciet niet te aggressief over wil komen. De verliezen zijn daarbij vooralsnog beperkt gebleven.

Een redelijke strategie in het licht van dreigingen is dus om vertrouwen in eigen (veer)kracht uit te blijven stralen en om alleen tegen de bad guys wantrouwend en gericht hard op te treden. En dus niet tegen iedereen!

[2] Volgens de wet computercriminaliteit II die sinds 2006 van kracht is kan een officier van justitie in een vroeg stadium een provider opdragen bepaalde telecommunicatiegegevens vast te houden die eventueel later pas opgevraagd worden.

Hoofdstuk 21

Eigen kluis & sluis

De grote vraag die bij het voorafgaande steeds speelt is hoe we individuen voldoende vrijheid, privacy en autonomie kunnen blijven garanderen in tijden waarin informatie en communicatie technologie vooral ingezet lijkt te worden voor verschuiving van de machtbalans in het nadeel van individuen. Een richting waar de grote partijen (overheden en bedrijfsleven) en ook individuen ieder voor zich voordeel van lijken te hebben is *personalisatie*. Via zo'n persoonlijke, op de menselijke maat toegesneden benadering van individuen kunnen overheden en bedrijven klantgerichter en effectiever opereren en worden individuen niet met ongerichte informatie en aanbiedingen overladen. Wat onderdeel van echte personalisatie zou moeten zijn is dat individuen ook echt serieus genomen worden, in hun verschillende rollen en kleinschalige verbanden, en ook elektronisch het beheer gegeven wordt over de eigen identiteiten en gegevens. Hierdoor blijft personalisatie niet beperkt tot eenrichtingsverkeer waarbij de grotere partij bepaalt wat voor een individu relevant is, maar waarbij het individu zelf (mede)bepaalt welke informatie op welk moment gepast is.

In dit hoofdstuk wordt een schets gegeven van hoe ICT positief ingezet kan worden om deze menselijke maat te bevorderen[1]. Het gaat hierbij nadrukkelijk om een schets die in dit stadium onvoldoende in detail uitgewerkt is om bij wijze van spreken morgen gerealiseerd te kunnen worden. De meeste technische ingrediënten ervoor zijn wel voor handen maar de totale samenhang (architectuur) en organisatorische en juridische inbedding is nog onvoldoende uitgewerkt. Concrete realisatie zal ongetwijfeld een aantal jaren vergen.

Dat hoeft ons er echter niet van te weerhouden om nu reeds concreet na te denken over een meer gepersonaliseerde en gedecentraliseerde ICT-infrastructuur die rekening houdt met gerechtvaardigde privacy eisen en zorgt voor persoonlijke veiligheid. Die infrastructuur wordt hier beschreven in termen van persoonlijke apparaatjes die een beperkt aantal persoonsgebonden functies vervullen: ze vormen tegelijkertijd een persoonlijke kluis voor gevoelige gegevens en een sluis voor communicatie met andere computers in de omgeving. Je kunt daarbij denken aan een veilige handpalm compu-

[1] Het is natuurlijk geenszins uitgesloten dat dit ook op andere wijze kan.

ter, ofwel *trusted personal digital assistant* (TPDA) met speciale programmatuur. Het apparaatje moet betrouwbaar zijn, voor alle partijen die ermee te maken krijgen.

Een mogelijk gebruiksscenario is het volgende. Stel u komt in een winkel en wil (alweer) een fles whiskey kopen. Daarvoor is het nodig dat u laat zien dat u boven de 18 jaar bent. U wil echter geen persoonsbewijs overhandigen omdat de winkelketen alles opslaat en het afgelopen jaar een aantal keer in het nieuws is geweest in verband met het verlies van klantenbestanden. U vindt eigenlijk zelf ook dat u iets te veel drinkt, maar u wil dat niet van anderen horen, en u wil dat zeker niet geregistreerd hebben in bestanden waar u zelf geen enkele controle over heeft. Wie weet wanneer het ooit eens naar boven komt. Maar u moet nog steeds laten zien dat u boven de 18 bent. Op dat moment haalt u uw TPDA te voorschijn en zendt u de winkelier draadloos een geanonimiseerd attribuutcertificaat, getekend door uw gemeente, waarin staat dat de houder boven de 18 is. De winkelier moet dan echter nog weten dat het certificaat echt van u is, en niet van uw veel oudere broer. De TPDA kan tonen over de geheime privé sleutel te beschikken die hoort bij het certificaat, via een *challenge-response* spelletje (zie Hoofdstuk 8). Dan nog zou de TPDA niet van u maar van uw oudere broer kunnen zijn. Maar hiervoor wordt nog een biometrische verificatie opgenomen, waarbij u even uw vinger legt op de vingerafdruklezer op de eigen TPDA. Alleen bij een match wordt de *challenge* ondertekend. Via dit mechanisme is iedereen tevreden: de winkelier heeft een bewijs van de vorm "de klant, wie het ook mogen zijn, is boven de 18" waarvoor u niks meer hoefde te doen dan op uw TPDA dit attribuut te selecteren en uw vinger op de ingebouwde lezer te leggen.

Het Burger Service Nummer (BSN) stoelt op het principe van eenmalige gegevensverstrekking: de burger mag niet gevraagd worden informatie op formulieren in te vullen die de overheid al heeft. Maar met een TPDA met persoonlijke gegevens is het elektronisch invullen van formulieren een eenvoudige kwestie: items selecteren en verzenden. De ontvangende partij kan de integriteit en authenticiteit automatisch controleren via elektronische handtekeningen. Via zo'n TPDA beheert de burger zelf de eigen gegevens en is een koppelingsmechanisme als het BSN helemaal niet nodig. De burger zelf staat centraal en vormt de koppeling.

Dergelijke scenario's zijn natuurlijk in veel meer situaties mogelijk, variërend van toegang tot gebouwen en openbaar vervoer tot aanvraag van allerlei voorzieningen. De TPDA moet de daarvoor benodigde (cryptografische) operaties veilig en betrouwbaar kunnen uitvoeren[2]. Hieronder worden een aantal eisen en mogelijkheden geschetst om een beter idee te geven.

Persoonsgebondenheid via *onboard* biometrie

Zoals in het voorbeeld scenario bevat iedere TPDA een ingebouwde biometrische lezer, zoals bijvoorbeeld een vingerafdruklezer[3]. Welk biometrisch kenmerk precies

[2] De TPDA vormt mijn zogenaamde *trusted computing base.*.

[3] Nu reeds zijn er PDAs met een biometrische lezer verkrijgbaar, maar niet met alle andere hier genoemde aspecten.

uitgelezen wordt doet er nu even niet zoveel toe. Het moet vooral sterk onderscheidend zijn, moeilijk na te maken, en niet achteloos in een andere situatie opgenomen kunnen—zoals bij een vingerafdruk op een glas. Via deze biometrie is mijn TPDA aan mij gebonden: mijn TPDA bevat—in elektronische vorm vastgelegd in beveiligde hardware—een biometrisch kenmerk van mij[4], van dezelfde soort als door de ingebouwde lezer opgenomen kan worden. Biometrische checks zullen vereist zijn voor cruciale operaties die door het apparaatje uitgevoerd worden, om er zeker van te zijn dat ik degene ben die de operatie accordeert.

Een wezenlijk aspect hierbij zal zijn dat de biometrische lezer integraal onderdeel is van de TPDA en dat de vergelijking tussen de onboard template en de vers gelezen template binnen het apparaatje plaats zal vinden. Vervolgens gaat er een 'groen' of een 'rood' lichtje branden; het geeft aan of er wel of niet een biometrische match plaatsvindt. Ook kan met het gaan branden van het groene lichtje een andere operatie—die authenticatie vereist—in gang gezet worden.

Het grote voordeel van deze onboard verificatie is dat ik mijn biometrische gegevens enkel aan mijn vertrouwde eigen apparaatje hoef te geven, en niet aan willekeurig welke biometrische lezer dan ook—van een bank, winkel, coffeeshop of ver buitenland—waarbij ik geen enkele duidelijkheid heb over het mogelijk oneigenlijke gebruik van de afgelezen template met mijn biometrische kenmerken. Een consequentie is dat niet alleen ik maar ook anderen het apparaatje moeten kunnen vertrouwen. Immers, bij een identiteitscontrole op straat of bij een grensovergang moet de controleur het 'groen' of 'rood' kunnen vertrouwen.

De werkelijk achterdochtigen zullen (terecht) opmerken dat ik mijn biometrische gegevens nog kwijt kan raken indien ik ze per ongeluk invoer op een andere TPDA dan de mijne. Dat klopt. Daarom is het zaak mijn TPDA goed bij me te houden. Het gaat om een waardevol stuk gereedschap in het digitale tijdperk.

Tegelijkertijd biedt deze biometrische functie bescherming tegen misbruik van mijn TPDA door anderen bij diefstal: het apparaat werkt gewoon niet voor een ander dan ik. Wel moet ik zelf voor een (regelmatige) backup van mijn TPDA zorgen, zodat bij verlies een vervangend (leeg) apparaatje met mijn eigen gegevens en sleutels geladen kan worden.

Beperkte verbinding en functies

Het grootste beveiligingsrisico is ongebreidelde functionaliteit. Fabrikanten zijn geneigd iedere keer meer mogelijkheden en functies aan hun hardware en software toe te voegen om daarmee de verkoop van nieuwe versies te stimuleren. Het is voor hen heel moeilijk om te zeggen: hier is een fantastisch apparaat, het is heel veilig, maar kan bijna niks! Toch is zo'n houding nodig voor kritische toepassingen.

De TPDA die hier voor ogen staat heeft dus ook maar beperkte mogelijkheden voor communicatie met de omgeving. Iedere verbindingsmogelijkheid vormt namelijk een

[4] In plaats van de template zelf kan ook een daarvan afgeleid geheim opgeslagen worden, als *template protection*.

risico op inbraak en introductie van kwaadaardige software. Het meest overzichtelijke is communicatie via aansluiting van een draadje of via plaatsing van de TPDA in z'n standaard (*cradle*). Iets meer gebruikersgemak kan geboden worden (maar direct ook meer risico) door draadloze communicatie, maar dan alleen voor gebruik op de zeer korte afstand via zogenaamde *Near Field Communication* (NFC). Daarbij moet de gebruiker de TPDA vlak voor een lezer houden om communicatie mogelijk te maken. Dat maakt ongewild en onbedoeld contact moeilijker.

Natuurlijk onstaat snel de vraag: kan ik met mijn TPDA bijvoorbeeld ook telefoneren, fotograferen, muziek luisteren of surfen? Het is beter de TPDA echt te beperken tot de persoonlijke beheerstaken met betrekking tot identiteiten, gegevens en policies. Bellen en zo hoort daar niet toe. Wat mogelijk wel zou kunnen is *via* de TPDA bellen waarbij de TPDA zorgt voor eigen beveiliging van de verbinding.

Elektronische handtekening zetten

Net als de huidige generatie PDAs zullen deze TPDAs kleine beeldschermpjes hebben. Tevens zit mijn privé sleutel voor het zetten van elektronische handtekeningen (zie Hoofdstuk 8) veilig opgeborgen in mijn TPDA. Ik kan dan met mijn TPDA documenten elektronisch ondertekenen. Wanneer ik de tekst van het document op het (betrouwbare) schermpje bekeken en gecontroleerd heb kan ik via de biometrische lezer en mijn privé sleutel het document ondertekenen.

Het is hierbij belangrijk dat de hele TPDA vertrouwd wordt. Dit is essentieel bij elektronische handtekeningen. Het vormt een problematisch punt bij handtekeningen op een PC via een privé sleutel op een chipkaart. Een kwaadaardig virus of een inbreker zou een ander document op het scherm kunnen tonen dan ter ondertekening naar de chipkaart gaat. Daarmee wordt het hele proces ondermijnd. Bij de TPDA zal dat niet lukken omdat het tonen en ondertekenen binnen hetzelfde (beperkte) vertrouwde domein plaatsvinden.

Identiteiten van anderen controleren

De TPDA heeft, net als zo ongeveer iedere computer, meer rekenkracht dan ik. De TPDA kan dan ook gemakkelijk cryptografische berekeningen uitvoeren, bijvoorbeeld om handtekeningen van anderen te controleren. Een TPDA kan dan bijvoorbeeld een elektronische agent herkennen. Het is een communicatiepartner die een politiecertificaat kan tonen en het bijbehorende *challenge-response* spelletje (zie Hoofdstuk 8) met goed gevolg kan afronden. Ik kan mijn TPDA dan bijvoorbeeld zodanig instellen dat iedere partij die zich als agent kan authenticeren automatisch ook op verzoek mijn identiteit mag zien en controleren. Dit kan onderdeel zijn van een e-identificatieplicht.

Ook kan ik via mijn TPDA bijvoorbeeld controleren of een geldautomaat waar ik voor sta wel echt is. Ook dat verloopt via een *challenge-response* en een certificaat van de bank in kwestie. Mogelijk moet mijn TPDA daarbij wel een recente, authentieke

black list controleren om er zeker van te zijn dat het certificaat van de geldautomaat nog wel geldig is—en daarmee of het niet om een automaat gaat die onlangs bij een kraak in z'n geheel meegenomen is.

Een andere mogelijkheid, zoals besproken in Hoofdstuk 14, is om deze TPDA te laten fungeren als een bewaker tegen het heimelijk uitlezen van RFIDs die ik bij me draag.

Op zo'n manier vormt mijn TPDA mijn sluis waardoor mijn communicatie met andere computers plaatsvindt. Voor gevoelige zaken gebruik ik mijn TPDA om eerst de identiteit van de andere partij te controleren.

Opslag van cruciale gegevens en sleutels

Voor het zetten van mijn handtekening met mijn TPDA moet mijn geheime privé sleutel erin zitten. Ook andere sleutels (of wachtwoorden) voor andere toepassingen kunnen er goed in opgeslagen worden, en alleen gebruikt worden in speciale situaties, met of zonder biometrische verificatie. Ook persoonlijke attributen over mij zoals 'ouder dan 18', 'inwoner van Nijmegen' of 'drager van een BE rijbewijs' kunnen erin opgeslagen worden, en bij passende gelegenheid aan de omgeving afgegeven worden om (identiteitsarme) transacties mogelijk te maken.

Naast zulke cryptografisch relevante zaken kunnen er ook gewone gegevens in opgeslagen worden, zoals bijvoorbeeld cruciale zaken uit mijn medische dossier. Die gegevens moeten versleuteld worden zodat ze bij verlies van mijn TPDA niet toegankelijk zijn voor anderen. Ontsleuteling zal bijvoorbeeld weer een biometrische verificatie vereisen. Voor noodsituaties zou het zo ingericht kunnen worden dat iemand die zich kan authenticeren als medicus toegang tot het dossier kan krijgen, om mij ook bewusteloos na een ongeluk adekwaat te kunnen helpen.

Natuurlijk hoeven niet al mijn gegevens op mijn TPDA zelf te staan. Het is voldoende wanneer de gegevens ergens anders, alleen voor mij bereikbaar, versleuteld opgeslagen liggen. De TPDA hoeft dan alleen de codes voor toegang en ontsleuteling te bevatten. In feite bestaan er al zulke beveiligde opslagmogelijkheden, bijvoorbeeld bij de ABN Amro bank (toegankelijk als bij internetbankieren) en bij `www.lockertje.nl` (toegankelijk via naam plus wachtwoord). Door combinatie met een TPDA kan zulke opslag nog veiliger.

Andere gegevens die ik bijvoorbeeld op mijn TPDA zou willen zetten kunnen eigen aankoop- en profiel-gegevens bij bepaalde winkelketens zijn die mij korting verschaffen wanneer ik ze bij binnenkomst van de winkel of bij het afrekenen toon. Op zo'n manier beheer ik mijn eigen kortingskaart. De gegevens kunnen tegen manipulatie beschermd worden met elektronische handtekeningen van de winkelketen.

Ook zou mijn TPDA gebruikt kunnen worden voor de aanhechting van policies (gebruiksbeslissingen) aan gegevens die ik aan de buitenwereld overgedraag, zodat (nette) ontvangende partijen zich aan mijn regels voor het gebruik van die gegevens kunnen houden.

Elektronisch geld

Het is een interessante uitdaging (geweest) in de cryptografie hoe elektronische muntjes georganiseerd kunnen worden. Gewoon een bestandje “deze file is één Euro waard” werkt niet als munt, omdat het eindeloos gekopieerd kan worden. Het is in het algemeen van belang dat elektronische muntjes herkend kunnen worden als echt, overdraagbaar zijn, niet twee keer uitgegeven kunnen worden, en liefst ook nog anoniem en niet-traceerbaar zijn. Er zijn inmiddels verschillende geschikte systemen uitgedacht waarbij bijvoorbeeld electronische muntjes in principe anoniem zijn behalve wanneer ze twee keer gebruikt worden: alleen bij zulk misbruik kan de identiteit van de eigenaar vastgesteld worden.

Hoe dit precies werkt voert hier te ver. Maar een TPDA vormt een mogelijke drager voor zulke elektronische muntjes waardoor anoniem betalen mogelijk blijft—zoals nu nog met kontante betalingen. Voor kleine betalingen, bijvoorbeeld op internet of bij tolstations, kunnen zulke elektronische munten erg handig zijn. Ze kunnen aanleiding geven tot nieuwe economische activiteiten.

Elektronische verkiezingen

Traditioneel verloopt stemmen via stembiljetten, bij landelijke verkiezingen of bijvoorbeeld ook bij verkiezingen voor een ondernemingsraad. De laatste jaren wordt in allerlei vormen geëxperimenteerd met elektronische verkiezingen via internet. Het is daarbij een grote uitdaging verschillende eisen te combineren: alleen stemgerechtigde kiezers mogen een stem uitbrengen, de vertrouwelijkheid van de uitgebrachte stemmen moet gewaarborgd zijn, en het moet duidelijk zijn dat de uitgebrachte stemmen ook inderdaad bijdragen aan het eindresultaat.

De afgelopen jaren zijn cryptografische technieken ontwikkeld die een uitweg bieden in dit spanningsveld. Daarvoor moeten kiezers enerzijds hun identiteit onmiskenbaar aan kunnen tonen, en anderzijds over betrouwbare eigen rekenkracht beschikken om de noodzakelijke cryptografische operaties te kunnen uitvoeren. Ook hier kan een TPDA een rol vervullen—beter dan een onbetrouwbare PC vol virussen. Uitgebreide experimenten zijn echter nodig om na te gaan of er voldoende garanties (technisch en organisatorisch) bestaan om ook zwaarwegende verkiezingen als voor de Tweede Kamer op een zodanige wijze te organiseren.

Openheid en onafhankelijke certificatie

Bij alle cruciale taken die hierboven voor een TPDA voorzien zijn is het duidelijk dat er groot en breed vertrouwen in de apparaatjes moet bestaan. Cruciaal daarvoor is dat er niet geheimzinnig gedaan wordt over wat er precies in zit en hoe het werkt. Daarom moet het ontwerp geheel open zijn en moet de software die erin zit openbaar beschikbaar zijn. Daarmee kan in principe iedereen de werking controleren. In de praktijk zullen maar weinig mensen dat daadwerkelijk doen. Maar het feit dat het

in principe mogelijk is is belangrijk voor het publieke vertrouwen: je kunt altijd een specialist inhuren die het voor je nakijkt.

Openheid heeft twee bijkomende positieve aspecten. De programmeurs die de software schrijven voelen dat hun beroepseer in het geding is en zullen dus veel zorgvuldiger werken dan wanneer hun programmatuur gesloten blijft. Daarnaast is de kans groter dat fouten sneller gevonden worden, waardoor verbeteringen ook vlot doorgevoerd kunnen worden.

Tenslotte moeten erkende onafhankelijke partijen zo’n TPDA certificeren voor officiële taken, zoals identiteitscontrole. Een deel van de certificaten zal van de overheid komen. Maar ook commerciële en andere partijen spelen hierbij een rol, bijvoorbeeld om je lidmaatschap van de tennisvereniging aan te tonen bij het online reserveren van een tennisbaan. Mogelijk kunnen hiervoor verschillende ingeklemde SIM-achtige kaartjes van vertrouwde partijen als interne *observer* gebruikt worden.

Het bovenstaande vormt een mogelijke manier om een ‘menselijke maat’ in ICT te realiseren, waarbij individuen centraal staan en in een redelijke machtsbalans leven met hun omgeving. Zoals eerder vermeld is zo’n balans een expliciete wens van de overheid in het programma ‘Andere Overheid’. Daartoe zal macht en informatie verdeeld moeten worden, op zodanige manier dat burgers er in vergaande mate zelf voor kunnen kiezen wanneer ze wat aan wie over zichzelf naar buiten brengen.

Literatuur

Hieronder worden enkele boeken genoemd die gebruikt kunnen worden voor verdere verdieping in het onderwerp. Bij een aantal relevante onderwerpen worden verwijzingen met een korte beschrijving gegeven, zonder enige claim op volledigheid.

Privacy

Het eerste boek is een klassieke verzamelbundel met veel belangrijke filosofische teksten (van voor 9/11), verschenen in een symbolisch jaar:

- F. Schoeman, editor. *Philosophical Dimensions of Privacy. An Anthology*. Cambridge Univ. Press, 1984.

Hetvolgende is een meer journalistieke beschrijving van de stand van zaken na 9/11, vooral in de Verenigde Staten:

- R. OHarrow Jr. *No Place to Hide*. Free Press, 2005.

Cryptografie

De eerste twee boeken hieronder zijn historische van aard, waarbij het eerste een omvangrijk standaardwerk is en het tweede een journalistieke beschrijving van de meer recente geschiedenis.

- D. Kahn. *The Codebreakers. The Story of Secret Writing*. Macmillan Publishing Co., 2^{nd} rev. edition, 1996.
- S. Levy. *Crypto. How the code rebels beat the government—saving privacy in the digital age*. Penguin Books, 2001.

De volgende twee boeken zijn sterk wiskundig, waarbij de tweede in het bijzonder gericht is op privacybeschermende technieken.

- G. Tel. *Cryptografie. Beveiliging van de digitale maatschappij*. Pearson Education, 2002.
- S. Brands. *Rethinking Public Key Infrastructures and Digital Certificates: Building in Privacy*. MIT Press, 2000. Gratis beschikbaar via `www.credentica.com`.

Beveiliging, met name van computers

De eerste twee boeken zijn beschrijvend en goed toegankelijk, waarbij het tweede ook ingaat op de gevolgen van 9/11. Het derde boek gaat iets meer in op technische aspecten, maar in brede zin.

- B. Schneier. *Secrets and Lies. Digital Security in a Networked World.* Wiley Computer Publishing, 2000.
- B. Schneier. *Beyond Fear. Thinking Sensibly About Security in an Uncertain World*. Copernicus Books, 2003.
- R. Anderson. *Security Engineering*. John Wiley & Sons, 2001. Gratis beschikbaar via `www.cl.cam.ac.uk/~rja14/book.html`

Overheid

De eerste drie boekjes geven vooral organisatieadvies.

- C. Prins and M. de Vries. *ID or not to be?* Rathenau Instituut, 2003.
- J. Reterink en M. Reuvers. *Werkbare vormen van digitale regie over eigen (persoons)gegevens door de burger*. Berenschot, 2003.
- P. Mettau. *mijnoverheid.nl*. Het Expertise Centrum, 2005.

Hieronder volgt eerst een boekje met algemene richtlijnen voor het privacyvriendelijk gebruik van ICT, en dan een met een beschrijving van wat er allemaal mis kan gaan, met name in de medische sector. Tenslotte wordt een uitgebreid en kritisch (engelstalig) rapport genoemd over plannen voor een nationale identiteitskaart in Groot-Brittannië.

- R. Koorn *et al*. *Privacy Enhancing Technology. Witboek voor beslissers*. 2003. Beschikbaar als `www.cbpweb.nl/downloads_technologie/Witboek_PET.pdf`.
- K. Spaink. *Medische Geheimen*. Nijgh & Van Ditmar/XS4ALL, Amsterdam, 2005.
- The Identity Project. An assessment of the UK Identity Cards Bill and its implications. London School of Economics, Juni 2005. Beschikbaar als: `http://is2.lse.ac.uk/idcard/identityreport.pdf`.