

De overheid verzamelt informatie over ons gedrag. Internetproviders bewaren gegevens. Cameratoezicht neemt toe. Google maakt filmopnamen van straten. We zijn onderworpen aan identificatieplicht, trajectcontroles en satellietfoto's. Zijn we nu toch op weg naar het 1984 van George Orwell?

Privacy anno 2009

Een kwart eeuw na Orwells 1984

Bas Savenije

Tot voor kort genoot de gemiddelde Nederlander relatief veel privacy: informatie over je privé-gedrag verspreidde zich zeer beperkt, tenzij je natuurlijk een *celebrity* was. En het was behoorlijk bewerkelijk om informatie over onbekende personen te verzamelen.

Nu kan iedereen eenvoudig worden bekeken, gefotografeerd of gefilmd. Meer en meer mensen hebben een mobiele telefoon met een camera. En iedereen kan eenvoudig informatie over de hele wereld verspreiden. Voor je het weet sta je op YouTube. Google heeft het zoeken naar informatie gedemocratiseerd; je hoeft geen specialist te zijn om over vrijwel iedereen informatie te vinden. Het lijkt alsof iedereen een bekende Nederlander is geworden.

Maar er is meer. De overheid en diverse bedrijven verzamelen met moderne technologieën informatie over ons gedrag. Vaak zijn die technologieën voor andere doeleinden ontworpen, bijvoorbeeld voor terrorismebestrijding. Ze hebben dus duidelijke pluspunten voor onze veiligheid of voor de volksgezondheid. Deze ontwikkelingen hebben echter ingrijpende gevolgen voor onze privacy. Onze verwachtingen op dat gebied moeten we behoorlijk bijstellen ten opzichte van enkele decennia terug. Deze verandering vindt als het ware sluipend plaats, er heeft geen brede discussie over voorzorgmaatregelen plaatsgevonden. Had Scott McNealy van Sun Microsystems met zijn uitspraak tien jaar geleden dan toch gelijk? "You have zero privacy anyway. Get over it."

Privacy wordt vaak omschreven als 'the right to be let alone'. Maar verschillende mensen hebben op verschillende momenten verschillende meningen over wat privé is. Het is geen kwestie van 'one size fits all'. Veel mensen, vooral jongeren, gebruiken het internet om allerlei min of meer intieme details over zichzelf aan de wereld prijs te geven. Ook dat plaatst de privacy in een ander daglicht, maar daar gaat dit artikel niet over. Het gaat om die interpretatie van privacy, waarbij het onderwerp van bepaalde informatie het recht behoudt over de verspreiding daarvan.

Persoonsgegevens opvragen

Sinds 1 januari 2006 geldt in ons land de Wet vorderen gegevens. Deze wet geeft politie en justitie bevoegdheden om persoonsgegevens op te vragen bij maatschappelijke instellingen en bedrijven, op basis van een bevel van de officier van justitie. En dit betreft niet alleen naam, adres en woonplaats, maar ook andere gegevens, zoals verkeersgegevens. Verdenking van betrokkenheid bij een misdrijf is hiervoor voldoende en de drempel om tot die verdenking te komen, wordt steeds lager.

Er valt heel wat op te vragen, want er ligt veel informatie over ons opgeslagen in uiteenlopende databases. Om met je mobiele telefoon een verbinding totstand te kunnen brengen, moet het netwerk weten waar de telefoon en dus de eigenaar zich bevindt.

Internetproviders hebben gegevens over ons zoek- en surfgedrag. Met behulp van cookies (informatie die een server naar een browser stuurt om deze bij een volgend bezoek weer terug te sturen) kan het surfgedrag worden bijgehouden. Webbugs maken het mogelijk vast te leggen wie een bepaald bericht heeft gelezen. En dan is er nog spyware, software die clandestien op een pc wordt geïnstalleerd om informatie over het gedrag van de gebruiker te verzamelen. Een zoekmachine weet op den duur alles van de gebruiker omdat hij alle individuele zoekvragen vasthoudt en zo een nauwkeurig beeld opbouwt.

In Nederland moeten telefoon- en internetgegevens anderhalf jaar worden bewaard. In Groot-Brittannië is dat een jaar, in Duitsland werd na een brede discussie besloten dat een half jaar genoeg was. Van internetproviders vraagt dat overigens de nodige voorzieningen, want het is niet mogelijk om spam (volgens sommige schattingen 90 procent van alle mailverkeer) hiervan uit te zonderen.

Cameratoezicht neemt hand over hand toe, in winkels en winkelcentra, bedrijven, pretparken, vliegvelden en stations. In het ADO-stadion in Den Haag hangen zoveel camera's dat het als het strengst beveiligde stadion ter wereld wordt



beschouwd. Dan hebben we ook nog de identificatieplicht, trajectcontroles en het tappen van satellietverkeer. De recherche kan de camerabeelden opvragen van Rijkswaterstaat en beveiligingsbedrijven. Er verschijnen oproepen aan burgers om filmpjes van misstanden bij de politie te deponeren. En Google maakt zonder waarschuwing gedetailleerde filmopnamen van straten ten behoeve van hun digitale atlas. Niemand loopt meer onopgemerkt over straat. In toenemende mate worden RFID-tags geplaatst in persoonlijke eigendommen en identiteitsdocumenten. Iedereen die over de benodigde apparatuur beschikt, kan bij deze gegevens komen. Pretparken kunnen op deze manier bijvoorbeeld het gedrag van bezoekers in het park volgen.

Kleinere vergrijpen

Veel van de bestaande technieken zijn ontwikkeld in het kader van de terrorismebestrijding. Maar er is een duidelijke trend waarneembaar dat de overheid die technieken ook gaat aanwenden voor kleinere vergrijpen. Men gebruikt infraroodcamera's in helicopters om wietplantages op te sporen. En satellietfoto's om naar verbouwingen zonder vergunning te zoeken.

In Rijssen-Holtten dragen agenten een cameraatje op hun fietshelm, waarmee personen kunnen worden herkend. De politie beschikt over camera's in surveillancewagens, maar de gefotografeerde nummers worden niet opgeslagen. De regiopolitie IJsselland ging in 2008 over de schreef door de kentekens van alle voertuigen op de A28 en A50 vast te leggen en te bewaren. Als rekeningrijden zou worden ingevoerd, gaan alle verkeersbewegingen buiten de bebouwde kom in een databank.

Een complicerende factor in de discussie over de toepassing van nieuwe technologieën zijn de voordelen die deze kunnen brengen. Niet alleen voor terrorismebestrijding maar ook voor andere vormen van misdaadbestrijding (een overvaller op een tankstation is aangehouden dankzij een opsporingsfilmpje op YouTube) of bijvoorbeeld de volksgezondheid. Individuele privacyrechten moeten daarbij worden afgewogen tegen het publiek belang.

De uitbraak van de infectieziekte Sars, enkele jaren geleden in Azië, had voorkomen kunnen worden als de onderzoekers toegang hadden gehad tot locatiegegevens van mobiele telefoons van besmette mensen.

Een voorbeeld waar recent discussie over is ontstaan, is het elektronisch patiëntendossier (EPD). Het EPD geeft zorgverleners toegang tot medische gegevens die nodig zijn om te helpen. Op dit moment betreft dit met name medicatiegegevens en een samenvatting van het huisartsendossier. Zorgverleners moeten toestemming vragen voordat zij het dossier kunnen inzien. De patiënt kan ook zelf met de huisarts bespreken welke informatie deze via het dossier met anderen mag delen. Je kunt controleren wie jouw dossier heeft

ingezien. Van iedereen wordt een EPD gemaakt, behalve van degenen die bezwaar maken. Tegenstanders hadden dat liever andersom gezien: alleen een EPD als je daarom vraagt.

Mens blijft zwakke schakel

Waar liggen de problemen? Een systeem kan technisch gezien nog zo veilig zijn, maar de mens blijft een zwakke schakel. Het kan voorkomen dat de betrokkenen (bijvoorbeeld artsen en medewerkers) slordig omgaan met hun inloggegevens, aan onbevoegden gegevens verstrekken of toeven aan hun eigen nieuwsgierigheid.

Een ziekenhuisdirecteur die zichzelf had moeten laten opnemen, ontdekte achteraf dat diverse ondergeschikten zijn medisch dossier hadden ingezien, zonder dat dat nodig was voor de behandeling. In een Amerikaans ziekenhuis werd een deel van de staf ontslagen dat aantoonbaar had zitten snuffelen in het dossier van onder andere Britney Spears. Medische details lekten zo uit naar de pers. Toen voetballer Robin van Persie van verkrachting werd verdacht, probeerden meer dan tweehonderd Rotterdamse agenten zijn dossier in te zien.

De Duitse discountketen Lidl gebruikte video-opnamen om het eigen personeel te bespioneren.

In deze gevallen is sprake van ontoelaatbare opzet, maar er kan ook sprake zijn van menselijke onzorgvuldigheid. Zoals de officier van justitie die zijn pc met daarop allerlei dossiers, aan de straat zette. In 2007 raakte de Britse belastingdienst in de post twee schijfjes kwijt met de persoonlijke gegevens (inclusief bankgegevens) van ruim zeven miljoen Britse families.

Helaas zijn er ook voorbeelden van ontoelaatbaar commercieel gebruik van gegevens. De sekstest op www.jeechteeleeftijd.nl werd tot begin 2009 gesponsord door een fabrikant van een erectiemiddel. Meer dan 60.000 Nederlandse mannen hebben vragen over hun seksueel gedrag beantwoord en de gegevens zijn doorgestuurd naar de fabrikant. Het bedrijf dat hiervoor verantwoordelijk was, verzamelde gegevens via tientallen websites die vaak zijn gekoppeld aan tv-programma's van SBS en RTL. Daaronder bevonden zich gegevens die volgens de wet niet mogen worden verwerkt, tenzij de burger daartoe uitdrukkelijk toestemming verleent.

Roep om krachtige staat

Een Canadese begrafenisondernemer wist beslag te leggen op een lijst met namen en adressen van personen bij wie kanker was vastgesteld. Hij nam contact op met een vrouw die op de lijst stond om haar *pre-paid funeral services* aan te smeren. In Duitsland dook een cd op met 17.000 namen, adressen en bankrekeningnummers die een medewerker van een callcenter stiekem op zijn werk had gekopieerd. In de klassieke rechtsstaat is iedereen onschuldig totdat het tegendeel is bewezen. In de moderne samenleving is het



begrip onschuld aan het verwateren, zoals Bart de Koning beargumenteert in zijn boek *Alles onder controle*. Onze samenleving laat zich in toenemende mate leiden door angst voor risico's. Dit geldt niet alleen voor terreur en misdaad, maar ook voor milieu, verkeer en gezondheid. Het onderling vertrouwen tussen burgers neemt af en de roep om een krachtige staat neemt toe.

In een risicosamenleving wordt afwijkend gedrag steeds minder getolereerd. En dat zie je terug in de manier waarop de overheid moderne technologieën inzet.

Wat men uit al die opgeslagen data wil halen, is bruikbare informatie om zo tot kennis te kunnen komen. Dat kan met behulp van datamining: krachtige computers combineren gegevens uit talloze databanken om verdachte patronen te herkennen.

Essentieel daarbij is *profiling*: het vaststellen van bandbreedtes waarbinnen gedrag nog als normaal te omschrijven valt. Maar nog afgezien van de vraag of de profielen niet teveel door paranoïde types worden vastgesteld, profi-

ling werkt niet. De prototypische terrorist bestaat niet. Voor terrorismebestrijding moet de betrouwbaarheid 100 procent zijn. Is het 99 procent, dan heb je bij 100 miljoen inwoners 1 miljoen terreurverdachten.

Intussen worden steeds meer gegevens verzameld. Na een aanslag willen politici steevast meer bevoegdheden en databanken voor de inlichtingendiensten. In de Verenigde Staten verzamelt men passagiergegevens van honderden miljoenen vliegtuigpassagiers om deze vijftien jaar te bewaren. Het probleem is echter zelden een gebrek aan informatie. Inlichtingendiensten beschikken in principe over voldoende informatie om de daden van Mohammed B. en die van de Hofstadgroep te zien aankomen. Maar dan moet men wel op het juiste moment de juiste analyse loslaten op de beschikbare informatie. Er lagen nog vele uren aan tapes over de Hofstadgroep waar men nog niet aan toegekomen was. In 1970 kon de BVD door het af luisteren van telefoons weten dat Molukkers van plan waren een trein te kapen. Ook toen werd de informatie niet op tijd gebruikt.

Niet duidelijk over gebruik

Nergens zijn zoveel toezichtcamera's als in Groot-Brittannië. Maar er is bij benadering niet genoeg menskracht om dit materiaal te gebruiken, nog afgezien van de vaak slechte kwaliteit van de beelden. Camera's brengen menigten in beeld maar helpen nauwelijks bij de opsporing. Ze kunnen nuttig zijn voor een reconstructie na een aanslag, maar voorkomen deze niet.

De vraag is gerechtvaardigd wat de meerwaarde is van het verzamelen van zo veel gegevens over onverdachte mensen. De overheid is ook niet duidelijk over het gebruik van de gegevens. In de VS staat een half miljoen mensen op een lijst van potentiële terreurverdachten. In 2006 moest een KLM-toestel rechtsomkeert maken omdat het niet werd toegelaten tot het Amerikaanse luchtruim. De redenen waarom zijn nooit onthuld. En in Nederland kan of wil de regering niet vertellen hoeveel telefoons worden afgeluisterd.

De stijging van de hoeveelheid verzamelde gegevens is veel groter dan de stijging in het aantal opgeloste misdrijven. Zoals Arthur Docters van Leeuwen, indertijd hoofd van de BVD, al zei: "Je vindt een speld niet sneller door de hooiberg groter te maken". Een conclusie dringt zich op: de burger ligt langs de meetlat van de overheid maar het is niet bekend welke meetlat.

In de jaren zeventig was er zoveel protest tegen de door de overheid geplande volkstelling, dat deze gedwongen was het hele plan af te blazen. Het is opmerkelijk hoe weinig interesse er in de huidige tijd bij het grote publiek is voor de genoemde ontwikkelingen. Men ziet de voordelen van de nieuwe technologieën, maar is zich niet bewust van de kosten en de nadelen. Men erkent dat vrijheden zo nu en dan moeten worden ingeperkt omdat er grotere belangen op het spel staan. En bovendien wordt er vaak aan toegevoegd: "Ik heb niets te verbergen". Merkwaardig genoeg ontstond er wel commotie toen de politie kentekens van alle voertuigen op de A28 en A50 wilde vastleggen en bewaren. En dit ging alleen maar over een voertuig, zonder dat bekend was wie er in zit. Meer kritisch gestemde volgers van de ontwikkelingen baart dit grote zorgen. "De publieke opinie is zo sterk voor meer controle dat een politiestaat niet ver is", aldus Rop Gonggrijp, medeoprichter xs4all.nl.

Een oud-student had in de jaren 1999-2001 meegewerkt aan een artikelenreeks in het *Ublad*, het blad van de Utrechtse universiteit. De artikelen staan nog altijd op de site van het blad en de student had gevraagd ze te verwijderen. Hij was bang dat de indertijd door hem geventileerde opvattingen hem nu schade zouden berokkenen. Het *Ublad* heeft geweigerd de teksten te verwijderen en kreeg daarin gelijk van de Raad voor de Journalistiek.

Facebook wisselde in 2007 gegevens van gebruikers uit met webwinkels: nu kon je van iedereen zien wat deze online gekocht had. Een Amerikaanse student ontdekte zo dat zijn

vriendin hem met een cadeautje wilde verrassen. Als gevolg van de vele protesten heeft Facebook deze dienst moeten beëindigen.

Een andere nieuwe dienst van Facebook: News Feeds. Zodra je je profiel op Facebook had gewijzigd, ging er automatisch een bericht naar je vrienden dat dit gebeurd was. Ook dit leidde tot veel klachten. Men wilde liever niet dat de wijzigingen aan de grote klok werden gehangen, men wilde het eigen profiel stilzwijgend 'verbeteren'. Het ging hier dus niet om geheimhouding; men wilde niet dat de toegankelijkheid van de informatie werd verbeterd.

Naarmate de risico's duidelijker worden, door incidenten zoals het in verkeerde handen vallen of misbruik, zal het draagvlak voor de maatregelen naar verwachting afnemen. In dit verband wordt vaak het volgende voorbeeld gebruikt. Gooi een kikker in een pan met heet water en hij springt er onmiddellijk uit. Warm je de pan rustig op dan blijft de kikker rustig zitten tot hij bezwijkt.

Noodzaak tot bescherming

Zijn we nu op weg naar Orwells 1984? Deze vergelijking gaat behoorlijk mank. De nieuwe technologieën worden als onderdeel van een rationeel proces ingezet voor een efficiënt bestuur, en niet, zoals bij Orwell, voor de macht van een elite.

In het verleden werd onze privacy beschermd door *practical obscurity*: de moeite die men moest doen om informatie te verkrijgen was meestal te groot om tot misbruik ervan te kunnen leiden. Het verkrijgen van informatie is echter aanzienlijk eenvoudiger geworden. Dit betekent niet per se dat we onze principes voor privacy ingrijpend moeten herzien. Het impliceert wel een sterk toegenomen noodzaak tot bescherming van onze privacy.

Natuurlijk kan de techniek die ten grondslag ligt aan de bedreiging van de privacy, ook worden ingezet voor de bescherming ervan.

Bekende technieken zijn:

Cryptografie: het opzettelijk versleutelen van informatie met behulp van een algoritme; slechts als men de methode kent en over de sleutel beschikt, kan men de boodschap ontcijferen.

Steganografie: het verbergen van een boodschap op een plaats waar anderen deze niet zo gauw zullen zoeken, bijvoorbeeld in een digitale foto of muziek.

Identificatie en authenticatie: bijvoorbeeld met username en password. Er zijn drie methoden tot authenticatie: met behulp van een eigendom (sleutel, smart card), met behulp van kennis (een password of een antwoord op een persoonlijke vraag), of met behulp van een onmiskenbaar deel van de persoon (biometrie: vingerafdruk, gelaat, iris). Belangrijk daarbij is uiteraard de vraag wie de authenticatie-informatie opslaat en bewaart.

In het algemeen geldt: hoe beter de beveiliging van een systeem is, des te lastiger is het te gebruiken en des te duurder is de administratie. Grote voorstanders van bewakings technieken gaan er vaak van uit dat het gebruik ervan van tevoren kan worden gedefinieerd en beperkt. Dat is echter niet het geval. Maar vaak is de technologie ook niet het probleem. In de eerste plaats zijn gebruikers zich vaak niet bewust van de risico's. Daarnaast moeten we ons goed realiseren dat alle technologie onderdeel is van een systeem met *administrators*, klanten, beleidsmakers, managers en veiligheidsadviseurs. Essentieel is dat het menselijk aspect van het systeem goed geregeld is, want juist daar blijkt het regelmatig fout te gaan.

Veel mensen gaan risico's tegemoet zonder dat ze het weten. Vooral beginnende gebruikers hebben vaak veel vertrouwen. De overheid zal de voorlichting over de maatregelen moeten verbeteren. Maar, zoals we hebben gezien, de problemen liggen niet alleen bij de overheid. Daarom zal in het onderwijs meer aandacht moeten zijn voor de risico's op het gebied van privacy die samenhangen met de informatisering.

Breed debat nodig

Wat bovenal nodig is, is een breed debat over privacy en veiligheid. Nu komen de maatregelen ad hoc en vindt er geen evaluatie plaats. Belangrijk is dat de overheid zich bewust is van haar dubbele rol. Als de overheid steeds meer gegevens opvraagt, hebben de burgers het recht om verantwoording te vragen over dit gedrag in de vorm van een evaluatie van de maatregelen met gedegen cijfers en analyses. Bij alle nieuwe maatregelen moeten tenminste de volgende aspecten expliciet aan de orde komen (zie ook de privacyregels van de Consumentenbond):

- Het doel van de maatregel moet helder en legitiem zijn.
- Het moet vaststaan dat de maatregel daadwerkelijk het geformuleerde doel dient.
- De gegevens mogen alleen gericht worden gebruikt voor het beoogde doel.

- Als het niet per se nodig is, moeten geen persoonsgegevens worden vastgelegd van wie dat niet wil.
- Mensen moeten controle hebben over hun eigen informatie.
- Er moeten garanties zijn voor een correcte manier van verwerken.
- Er moet een goede voorlichting zijn over de maatregel.
- Er moet een regeling zijn voor toezicht en evaluatie.

In 1787 bedacht de filosoof Jeremy Bentham een ideale gevangenis, een zogeheten *panopticon*. Iedere gevangene zou permanent kunnen worden geobserveerd zonder te weten op welk moment hij daadwerkelijk geobserveerd werd. Er zijn voldoende argumenten die erop duiden dat deze vergelijking, net als die met Orwells 1984, mank gaat en dat ons perspectief aanzienlijk rooskleuriger is. Maar die realiteit komt niet vanzelf. **IK**

Bas Savenije is algemeen directeur van de Koninklijke Bibliotheek. Hij schreef dit artikel op persoonlijke titel.
– b.savenije@uu.nl

(advertentie)

Het beste van HBO en wetenschap.



Scriptiewinkel.nl