NJB, Focus, Afl. 2007/37, 19 oktober 2007, www.njb.nl.

GLAZEN SAMENLEVING IN ZICHT

Jacob Kohnstamm is voorzitter van het College bescherming persoonsgegevens en Lynsey Dubbeld is daar werkzaam als beleidsmedewerker.

Leven we in een glazen samenleving? Dat wil zeggen, spelen hightech-gegevensverwerkingen die ons gedrag als burgers en consumenten transparant maken een hoofdrol in onze samenleving? Er zijn aanwijzingen dat een 'glazen samenleving' in zicht komt. Wat betekent dat voor individuen en de maatschappij, welke risico's doen zich voor, en wat is er tegen de nadelige effecten te doen?

Vrijwel dagelijks zijn er nieuwe voorbeelden te vinden van verregaande verwerkingen van persoonsgegevens. Sla er alleen al eens de kranten op na: de berichten over overheidsplannen voor een betere dienstverlening aan de burger, uiteenlopende methoden van dataverzameling in de private sector en voortdurende uitbreiding van elektronisch cameratoezicht vliegen je om de oren. En dan zijn er ook nog allerlei technische innovaties, in binnen- en buitenland, die in de nabije toekomst een breed gebruik kunnen krijgen.

In de publieke sector zijn dit jaar de nodige stappen gezet die de komst van een glazen samenleving dichterbij brengen.

De Eerste Kamer stemde in juli in met het wetsvoorstel dat de invoering van het burger servicenummer (BSN) regelt. Het 'sofinummer nieuwe stijl' wordt een identificatienummer dat door een veelheid aan overheidsorganisaties wordt gebruikt als instrument in de strijd tegen administratieve regeldruk. Het beoogt administratieve fouten te verminderen, klantgerichte dienstverlening te verbeteren en betere bescherming te bieden tegen identiteitsfraude. Voor burgers betekent het BSN dat ze in beeld blijven bij allerlei overheidsdienstverleners, terwijl het risico bestaat dat er onjuiste gegevens over hen worden uitgewisseld.

In de zogenaamde SUWI-keten is inmiddels een digitaal klantdossier in het leven geroepen, waaraan diverse bij uitkeringen betrokken instanties bijdragen. Over cliënten van UWV, CWI, reïntegratiebureaus en gemeentelijke sociale diensten worden gegevens gekoppeld en uitgewisseld. Op termijn zal dit klantdossier uitgroeien tot een veelomvattend klantvolgsysteem binnen de keten.

De overheid let ook op de kleintjes. Vanaf januari 2008 krijgt ieder kind in Nederland een elektronisch dossier, het EKD. Met de komst van het EKD wordt voor alle kinderen tussen nul en negentien een dossier aangemaakt op het moment dat ze met jeugdgezondheidszorg in aanraking komen. Naast het EKD wordt gewerkt aan een landelijke Verwijsindex Risicojongeren: met dit aparte programma kunnen hulpverleners zien welke andere instanties, waaronder Bureau Jeugdzorg, huisartsen, politie en justitie, zich bezighouden met een jongere uit deze categorie.

Ook in het bedrijfsleven worden steeds vaker technieken ingezet die in staat zijn een overzicht te creëren van een persoon en diens omgeving, handelingen en relaties. Google gaat daar waarschijnlijk het verste in. De zoekmachine bewaart alle zoekgegevens van gebruikers, gebruikt cookies met een lang leven en scant e-mails van gebruikers van G-mail met het oog op gerichte marketing.

Voor reclamedoeleinden doen ook andere bedrijven gekke dingen. Zo hebben 5000 Nederlanders met een inkomen van minimaal tweemaal modaal eerder dit jaar van Robeco een luchtfoto ontvangen met daarop hun eigen huis en de vraag: '10,66 procent rendement, zit ú in de buurt?' Robeco gebruikte namen en adressen uit eigen bestanden die voor de reclame met andere databestanden zijn gekoppeld. De foto's zijn vervolgens gemaakt door een luchtfotobedrijf. In het buitengebied bij Zutphen zorgde de reclame voor discussie: wie was dan wel die buurman met dat hoge rendement?

Een voetbalbond heeft persoonsgegevens van een jeugdvoetbalvereniging verkocht voor commerciële doelen. Ouders van de voetballertjes werden telefonisch benaderd door een voetbaltijdschrift en ook andere bedrijven (waaronder uitgeverijen en een telecom-aanbieder) bellen ouders met reclame. In een aantal gevallen werd naar geheime telefoonnummers gebeld.

De surveillance van nu heeft niet alleen te maken met dataverwerking door de overheid en het bedrijfsleven, maar ook met allerlei elektronische ogen die burgers in beeld brengen. Vooral voor doeleinden zoals veiligheid en beveiliging - een aspect van de glazen samenleving met een status aparte dat we hier voor de volledigheid toch noemen - doen zich veelzeggende ontwikkelingen voor. Camera's kunnen bijvoorbeeld steeds meer. Rond station Vlaardingen hangen twee sprekende camera's. Vanuit een centrale meldkamer kunnen overlastgevers worden toegesproken door medewerkers van ProRail. De bedoeling is mensen af te schrikken. In het Verenigd Koninkrijk wordt al in twintig gemeenten gebruikgemaakt van sprekende camera's.

Maar camera's kunnen ook luisteren. In het centrum van Groningen zijn elf van de camera's op straat

uitgerust met microfoons, die signalen van agressie detecteren. En camera's worden steeds slimmer. In Heerlen worden bedrijventerreinen en een autoboulevard beveiligd met camera's die in Born worden uitgekeken. De centrale meldkamer aldaar bekijkt beelden die worden geactiveerd als er iets afwijkends wordt geconstateerd. Vanaf afstand kunnen vervolgens lampen worden aangedaan, poorten geopend en via luidsprekers personen worden aangesproken.
Camera's worden vaker gebruikt in combinatie met andere hightech-controlesystemen, bijvoorbeeld in voetbalstadions waar in de toegangssluizen met behulp van biometrische controle (een gezichtsherkenningsysteem) nagegaan wordt of een persoon een stadionverbod heeft.
De ontwikkelingen op het gebied van surveillancesystemen staan niet bepaald stil.
Met Street View van Google kan je virtueel wandelen door straten in de VS. Voor deze tool zijn miljoenen foto's gemaakt via de camera's op het dak van een auto. Met de Street View-functie zijn mensen herkenbaar in beeld: meisjes in bikini en een man die een stripclub uit komt zijn al op de foto gezet. Vooralsnog is het virtuele ommetje alleen mogelijk in Miami, Denver, New York, San Francisco en Las Vegas, maar bij succes worden meer steden in beeld gebracht.
Het is de bedoeling dat in 2009 in het gehele Nederlandse openbaar vervoer de OV-chipkaart wordt ingevoerd ter vervanging van de trein- en strippenkaart. De NS belooft de reiziger extra gemak en minder zwartrijders. De persoonsgebonden OV-chipkaart houdt bij waar en hoe laat je in- en uitstapt en vormt dus een breuk met de huidige, anonieme manier van reizen. De NS wil onze gegevens jarenlang opslaan voor 'serviceverlening aan de klant'. Lees: marketingdoeleinden.
In nieuwe auto's in 25 Europese landen komt vanaf 2010 een automatisch handapparaat (E-call) dat aan de hand van sensoren weet of een auto ergens tegenaan is gereden en vervolgens automatisch een alarmnummer belt. De mogelijkheden van E-call lijken onbeperkt: het alarmnummer kan bijvoorbeeld bellen met de zorgverzekeraar van de bestuurder, zodat medische gegevens naar hulpdiensten worden verstuurd. Luxere toepassingen zijn ook al voorzien: de auto kan automatisch bellen naar de garage voor een onderhoudsbeurt of naar Wegenwacht bij pech onderweg.
De verwachting is dat de huidige generatie internettechnologieën in combinatie met identificatie- en sensortechnologieën en kunstmatige intelligentie vorm gaan geven aan een zogenaamde 'ambient intelligence wereld', een wereld waar wij omringd zullen zijn door intelligente systemen die kunnen reageren en anticiperen op onze wensen en behoeften. Dit betekent dat de bewegingen van een persoon of een object van die persoon door de fysieke wereld informatiesporen achterlaten in cyberspace. Die digitale voetstappen zijn voer voor surveillance.
Bovenstaande voorbeelden maken duidelijk dat op allerlei terreinen - verkeer en vervoer, overheidsdienstverlening aan de burger, marketing, internetgebruik, recreatie, jeugd en onderwijs - privacygevoelige monitoring plaatsvindt. Vaak gebeurt dit met de beste bedoelingen en voor prima doeleinden. Maar als je de verschillende ontwikkelingen in samenhang bekijkt, dan doemt toch het beeld op van een glazen samenleving waarin je nauwelijks meer onbespied door het leven kunt gaan.

Een glazen huis

Werden maatschappelijke ontwikkelingen die inbreuken op de persoonlijke levenssfeer meebrengen vroeger nogal eens in termen van Big Brother gevat, tegenwoordig wordt er meestal gesproken over een surveillance society.[1] In rijke westerse landen is het dagelijkse leven 24 uur per dag doordrenkt met doelgericht, systematisch, routinematig, vaak onopvallend toezicht.[2] Steeds vaker zijn geluiden hoorbaar dat het met deze controle uit de klauwen aan het lopen is. Eerder dit jaar vergeleek de Britse Information Commissioner, Richard Thomas, de onopvallende, sluipende inbreuk op burgerrechten die surveillance meebrengt met het langzaam koken van een kikker die - zonder dat hij het doorheeft - tot moes verwordt.[3]
Omdat er op allerlei terreinen van het dagelijkse leven zoveel persoonlijke informatie over vrijwel ieder van ons wordt vastgelegd, karakteriseren wij de hedendaagse Nederlandse samenleving in termen van een glazen huis.[4] In zo'n glazen samenleving wordt individueel gedrag uitvoerig gemonitord en wordt het persoonlijke leven steeds transparanter. We worden ongemerkt omgeven door wolken van digitale persoonsgegevens, die ieder afzonderlijk misschien niets zijn om de wenkbrauwen over op te trekken maar die in samenhang ervoor zorgen dat individuen zich in een minder vrije situatie bevinden.
Een glazen samenleving wordt meer realiteit naarmate onze maatschappij meer van de volgende kenmerken vertoont.
Ten eerste speelt technologie die een verwerking van persoonsgegevens met zich meebrengt een hoofdrol in het maatschappelijk functioneren. Het Global Positioning System, Radio Frequency Identification en biometrie zijn bijvoorbeeld geen toekomstmuziek meer.
Het zwaan-kleef-aan-effect dat nogal eens optreedt bij het gebruik van digitale systemen heeft tot

gevolg dat gemakkelijk data van de ene setting naar de andere stromen. Dat gebeurt vooral in het kader van samenwerkingsverbanden (bijvoorbeeld met het oog op bemoeizorg) en door bestandskoppelingen (zoals op het gebied van fraudebestrijding in de sociale zekerheid).
Ten tweede is typerend voor de glazen samenleving dat de toepassing van technologie plaatsvindt met de beste bedoelingen en samenhangt met een streven naar rationalisatie en efficiency. Bijvoorbeeld: de overheid beoogt met het BSN betere dienstverlening aan de burger en een efficiëntere overheidsadministratie te realiseren. Maar met het BSN weet de overheid straks wel alles over de contacten die we hebben met allerlei overheidsinstanties.
Ten derde treedt bij dergelijk gebruik van technologie nogal eens 'function creep' op: het bedoelde gebruik van bepaalde gegevens verschuift naar een nieuwe toepassing. Beveiligingscamera's blijken bijvoorbeeld niet alleen te worden gebruikt voor misdaadbestrijding maar ook voor de aanpak van zwerfafval. 'Function creep' kan ook betekenen dat technologieën die aanvankelijk gericht zijn op een specifieke (minderheids)groep langzamerhand worden toegepast op bijna iedereen. Bewakingscamera's zijn tegenwoordig niet alleen in gebruik om in winkels tasjesdieven in beeld te brengen, maar verschijnen overal op straat.
Ten slotte is er in een glazen samenleving in hoge mate sprake van 'social sorting': databanken worden geanalyseerd en gecategoriseerd om doelgroepen en risicogroepen te definiëren en daarvoor specifieke strategieën (op het gebied van marketing, dienstverlening, fraudebestrijding, enz.) te ontwerpen.[5] Zo ontvangen consumenten in (volgens de analyse van postcodegebieden) welgestelde stadsdelen aanbiedingen voor een voordelige verzekering, terwijl inwoners van zogenaamde achterstandswijken hogere premies betalen omdat zij voor verzekeraars een groter betalingsrisico met zich mee zouden brengen.[6]
Dit alles leidt ertoe dat de ('gewone') burger in het dagelijkse leven steeds minder onbespied blijft.[7] De keerzijde van onze efficiënte, mobiele, high tech-samenleving is dat vrijwel overal je doen en laten wordt gemonitord. Het persoonlijke leven is daardoor steeds meer een glazen huis waar nauwelijks gordijnen voor hangen.

Gevaren in een glazen samenleving

De glazen samenleving leidt niet simpelweg tot een niet nader omschreven inbreuk op de persoonlijke levenssfeer. Er doen zich, zo kan ook worden afgeleid uit de literatuur, in een glazen samenleving grofweg twee soorten problemen voor: praktische risico's, die vooral te maken hebben met informatiebeveiliging en datakwaliteit, en effecten die minder tastbaar zijn en meer fundamentele aspecten van onze maatschappij betreffen. Een glazen samenleving wordt zorgwekkender naarmate deze problemen frequenter en grootschaliger optreden.
De toename in datastromen, 'function creep', de alomtegenwoordigheid van surveillancetechnologie en het goedbedoelde streven naar efficiency vergroten de risico's op het gebied van incorrecte gegevens - met alle vervelende gevolgen van dien. Met het BSN wordt een eenmalig verkeerd geregistreerde geboortedatum, salarishoogte of adreswijziging tientallen keren doorgekoppeld aan andere instanties. En dat kan grote gevolgen hebben voor iemands uitkering, belastingaangifte of huursubsidie.
Daarnaast nemen de (gevolgen van) problemen met informatiebeveiliging toe. Dergelijke beveiligingsproblemen doen zich nu al regelmatig voor, zoals blijkt uit berichten in de media. We noemen enkele Nederlandse voorbeelden. In mei 2007 bleek dat alarmmeldingen voor brandweer- en ambulancediensten onbeveiligd worden rondgestuurd en vervolgens door websites zoals www.alarmeringen.nl worden gepubliceerd. Als gevolg hiervan is van de websites adresinformatie af te leiden over blijf-van-mijn-lijf-huizen. Ook datingsite Lexia kampte dit jaar met een beveiligingsprobleem. Een link in een doorgestuurde uitnodiging voor een singlefeest gaf volledige toegang tot het profiel van de afzender. Er kon vervolgens in de reacties van de profielhouder worden gelezen, foto's konden worden verwijderd of vervangen en het profiel kon worden aangepast. Een rechercheur van de KLPD is in het eerste weekend van juni zijn laptop kwijtgeraakt, waardoor politiegegevens op straat zijn komen te liggen. Niet de eerste keer dat zoiets in politie- en justitiekringen gebeurt.
In de glazen samenleving, waarin door technologie gefaciliteerde datastromen zo'n belangrijke rol spelen, wordt het risico op misbruik van persoonlijke informatie steeds groter. De praktijkervaring van specialisten leert dat de grootste bedreiging voor beveiliging niet voortvloeit uit ongeautoriseerde toegang tot persoonlijke informatie, maar uit misbruik van persoonsgegevens door geautoriseerd personeel.[8]
Ook identiteitsroof wordt in een glazen samenleving een punt van zorg. Fraude met paspoorten en andere identiteitsbewijzen neemt toe. Hoewel de nieuwe paspoorten en identiteitsbewijzen, die een

chip bevatten met foto en persoonsgegevens, moeilijker te vervalsen zijn dan de oude, bedenken criminelen steeds andere manieren van fraude.
In meer algemene zin kan het glazen huis gevolgen hebben voor een aantal fundamentele aspecten van onze samenleving.
De ontwikkelingen op het gebied van 'social sorting' creëren het risico van sociale uitsluiting en discriminatie. Het categoriseren van individuen en groepen op basis van datamining of andere analysen van persoonlijke informatie heeft invloed op de maatschappelijke verdeling van levenskansen. Waar je woont, wordt bijvoorbeeld bepalend voor welke lening, beveiliging en reclame je krijgt en welke bank of supermarkt er in de buurt gevestigd wordt.
Het uitvoerige toezicht op grote groepen burgers kan daarnaast gevolgen hebben voor (het gevoel van) autonomie van individuen. Wie zich bewust is van het geheel aan controlemechanismen op internet, op straat en aan het overheidsloket, zal al snel geneigd zijn tot het vermijden van afwijkend gedrag - om nóg meer surveillance te voorkomen, of om te voorkomen dat er verkeerde conclusies worden getrokken op basis van die surveillance. Uit onderzoek van EPN bleek onlangs bijvoorbeeld dat één op de tien geënquêteerden niet blij is met het beeld van zijn of haar persoon dat wordt geschetst op basis van internetvondsten.[9]
Ook bestaat de mogelijkheid dat een glazen samenleving gepaard gaat met een maatschappelijk klimaat van angst en wantrouwen. Een bespiede burger kan makkelijk een schichtige burger worden, zo kan worden geredeneerd. Het vertrouwen van de burger in de overheid als het gaat om het zorgvuldig beheren van persoonsgegevens staat nu al onder druk. Critici van het EKD zijn bijvoorbeeld van mening dat met de komst van het kinddossier elk gezin verdacht wordt gemaakt. Dat is geen goed nieuws voor een overheid die het vertrouwen van haar burgers wil koesteren.
Tot slot leidt de hoge mate van informatisering van de glazen samenleving tot een gebrek aan transparantie. Surveillancepraktijken vinden vaak buiten het zicht van de betrokkenen plaats. Daardoor neemt de weerbaarheid van burgers af, en raken de uitoefening van individuele rechten en het afdwingen van accountability bemoeilijkt. Het is geen eenvoudige opgave om het recht op inzage, waarin onder andere de Wet bescherming persoonsgegevens (Wbp) voorziet, uit te oefenen als je niet weet welke organisatie wat voor een soort gegevens over je verwerkt.

Gordijnen in het glazen huis

Uit het bovenstaande kan geconcludeerd worden dat de monitoring van het gedrag van burgers en consumenten op verschillende maatschappelijke terreinen - natuurlijk naast allerlei voordelen ten aanzien van serviceverlening, efficiëntie, veiligheid enz. - risico's en neveneffecten met zich meebrengt die vragen om een (re-)actie.

Wat kunnen burgers doen om hun glazen huis van enige gordijnen te voorzien?
Wij zijn van mening dat het denken over privacy een aantal beginselen heeft opgeleverd die bijdragen aan het inzichtelijker maken van surveillance. Dergelijke uitgangspunten voor een fatsoenlijke omgang met persoonsgegevens kunnen een tegenwicht bieden tegen het gebrek aan transparantie van gegevensverwerkingen waarmee burgers in de glazen samenleving worden geconfronteerd.
Burgers over wie persoonsgegevens worden verwerkt ('betrokkenen' in het jargon van de privacywet) hebben namelijk een recht op inzage, correctie, aanvulling en verwijdering. Daarmee kunnen ze inzicht krijgen in de gegevens die over hen worden verwerkt en hebben ze mogelijkheden om gegevensverwerkingen te veranderen of verminderen.
Voor organisaties en bedrijven die persoonsgegevens verwerken, geldt een informatieplicht. De voor de gegevensverwerking verantwoordelijke is verplicht om betrokkenen te informeren over wat er met hun persoonsgegevens gebeurt. Op deze manier kunnen burgers op de hoogte worden gesteld van de identiteit van de gegevensverwerker en het doel of de doeleinden waarvoor deze de gegevens verzamelt. In sommige situaties dient de betrokkene ook informatie te ontvangen over het gebruik van de persoonsgegevens. Deze informatie maakt burgers bewuster van datastromen en stelt ze beter in staat om zo nodig hun recht op inzage en recht op correctie, aanvulling en verwijdering uit te oefenen.
Individuen kunnen zich bovendien tot op zekere hoogte beschermen tegen weetgierige overheden en bedrijven. Het basisprincipe is: geef nooit meer informatie dan strikt noodzakelijk. Vooral op internet is de verleiding groot om persoonsgegevens af te staan, bijvoorbeeld door het invullen van contactformulieren.
Op internet is naar ons oordeel ook wat te winnen. Een zoektocht op internet kan je anoniem ondernemen, bijvoorbeeld via www.torr.eff.org. Ixquick is een zoekmachine die privacyvriendelijkheid

hoog in het vaandel heeft. Zoekmachine Ask.com introduceert later dit jaar een mogelijkheid om volledig anoniem te zoeken: AskEraser.

Wat mogen burgers en consumenten van het bedrijfsleven vragen?
Een basisbeginsel voor de zorgvuldige omgang met persoonsgegevens is: bepaal nauwkeurig het doel van een gegevensverwerking en neem daarbij de noodzaak van de verwerking (dat wil zeggen de proportionaliteit en subsidiariteit) in ogenschouw. 'Privacy mindedness' vereist onder meer dat bij de verwerking van persoonsgegevens de doeleinden worden gespecificeerd. 'Function creep' kan in hoge mate worden voorkomen als bedrijven en instellingen doelspecificatie serieus nemen.
Naast doelspecificatie is dataminimalisatie een uitgangspunt voor het tegengaan van de nadelige effecten van een glazen samenleving. Dat wil bijvoorbeeld zeggen: liever op risicotijden een beveiliger op de hoek van de straat dan permanent camera's in de hele stad. En als cameratoezicht dan toch moet, dan bij voorkeur intelligente camera's die alleen aan gaan als er iets ongebruikelijks wordt waargenomen.
Dataminimalisatie kan in veel gevallen worden ingebouwd in informatie- en communicatietechnologie (ICT) met behulp van Privacy Enhancing Technologies (PETs).[10] PETs zijn te omschrijven als een coherent systeem van ICT-maatregelen die privacy beschermen door het verwijderen of verminderen van persoonsgegevens of het voorkomen van onnodige/onwenselijke verwerkingen van persoonsgegevens. Er bestaan verschillende soorten PETs, ieder met een eigen, specifieke functie. Bijvoorbeeld identiteitsbeschermers (te gebruiken bij bijvoorbeeld anonieme klantenkaarten of prepaid telefoonkaarten) en versleuteling (waarmee het risico op ongeautoriseerde toegang tot gegevens kan worden verminderd).
Naast PETs zijn er, blijkens een recente studie van de Engelse Royal Academy of Engineering, verschillende technologische ontwikkelingen die kunnen bijdragen aan het verminderen van risico's op het gebied informatiebeveiliging.[11] Een belangrijk basisbeginsel is volgens de techniekdeskundigen het specificeren van het doel van het systeem zodat er een zo eenvoudig en direct mogelijke functionaliteit kan worden ontworpen, hetgeen complexiteit en dus kwetsbaarheden en fouten vermindert. Daarnaast kan een risicoanalyse vruchten afwerpen, zodat potentiële kwetsbaarheden kunnen worden geïdentificeerd en kan worden besloten welke strategieën nodig zijn om ze te beperken.
Voor de beveiliging van databases wordt in het rapport een verzameling relatief eenvoudige principes beschreven, zoals: sla data op in versleutelde vorm, corrigeer fouten snel, bewaar een minimum hoeveelheid gegevens voor een minimale tijdsduur, controleer regelmatig de juistheid van gegevens en zorg voor snelle informatie en compensatie aan betrokkenen wanneer gegevens kwijtraken.
Ten slotte wordt er wereldwijd hard gewerkt aan manieren om organisaties al vóór de introductie van nieuwe systemen te laten nadenken over nadelige privacyeffecten en privacyvriendelijke werkwijzen. Aan de hand van een inventarisatie van datastromen in en rond (al dan niet toekomstige) systemen kunnen organisaties hun innovaties relateren aan breed gedragen privacybeginselen (zoals doelbinding, informatieplicht, richtlijnen voor bewaartermijnen). In Canada zijn dit soort toetsen verplicht voor alle nieuw in te voeren overheidssystemen.

In hoeverre kan de overheid bijdragen aan fatsoenlijke informatieverwerking?
De Nederlandse vereniging voor internetprofessionals, Internet Society (ISOC) heeft de overheid opgeroepen niet langer externe 'spionagetools' te gebruiken op overheidswebsites.[12] Overheden en publieke diensten schakelen steeds vaker de diensten in van bedrijven zoals Nedstat, Google Analytics, Webtrends en Core Metrics. Een bezoeker van een overheidswebsite wordt daardoor vaak onmerkbaar en zonder waarschuwing geprofileerd op klikgedrag, waarbij ook elders verzamelde demografische gegevens worden gebruikt. ISOC stelt dat burgers er recht op hebben dat commerciële ondernemingen niet over hun schouder kijken als zij overheidsinformatie bekijken. Er zijn bovendien alternatieven: per website kunnen analysetools worden gedraaid en er kan kwalitatief naar sites worden gekeken via gebruikerspanels of 'usability experts'.
Van een fatsoenlijke overheid mag ook worden verwacht dat ze haar eigen informatiebeveiliging op orde heeft. Waarborgen voor een zorgvuldige omgang met persoonsgegevens kunnen ook maatregelen betreffen die op dit moment (nog) niet in regelgeving zijn opgenomen. Te denken valt aan het inrichten van aanspreekpunten voor vragen en klachten, het ontwikkelen van best practices, het instellen van audits, en het openbaar maken van auditresultaten. De overheid zou in dit opzicht een voortrekkersrol kunnen vervullen.
De overheid kan bovendien de technische creativiteit van bedrijven en instellingen bevorderen om op die manier technische oplossingen - die gezien de belangrijke rol van technologie in de glazen samenleving kunnen worden beschouwd als een topprioriteit - te stimuleren. Zou het bedrijfsleven met

een steuntje in de rug niet enthousiast kunnen worden voor de marktintroductie van bijvoorbeeld de door Latanya Sweeney ontworpen Identity Angel?[13] Deze webapplicatie verwerkt informatie die op internet wordt verzameld en verrijkt deze met andere publiek toegankelijke data. De software controleert op die manier of er met openbare bronnen zodanige informatie bijeen kan worden gesprokkeld dat iemand het slachtoffer kan worden van creditcardfraude. Het slachtoffer ontvangt vervolgens (zo mogelijk) een e-mailbericht met de gevonden informatie, zodat er maatregelen ter voorkoming van fraude kunnen worden genomen.
Tot slot kan de (beteugeling van de) glazen samenleving gebaat zijn bij een parlementair onderzoek naar de maatschappelijke effecten van de huidige surveillancepraktijken. In Engeland staat zo'n onderzoek al op stapel.

Privacydag

Zoals uit het voorgaande al blijkt, neemt de behoefte aan creatieve oplossingen voor de bescherming van de persoonlijke levenssfeer toe naarmate de glazen samenleving meer in zicht komt. Tegelijkertijd komt de naleving van de privacywetgeving, in het bijzonder op het gebied van de bescherming van persoonsgegevens, onder druk te staan. In een glazen samenleving bestaat immers het risico dat voorheen afzonderlijke gegevensverzamelingen met elkaar in verband worden gebracht en daardoor omvattender worden dan bij de invoering van de Europese dataprotectierichtlijn is voorzien.
Om verregaande inbreuken op de persoonlijke levenssfeer tegen te gaan en normontwikkeling in de glazen samenleving in goede banen te leiden kan het daarom nodig zijn om het bestaande dataprotectieregime te vernieuwen, bijvoorbeeld wat betreft het handhavingsinstrumentarium van de privacytoezichthouders.
De huidige handhavende bevoegdheden van Europese dataprotectie-autoriteiten vloeien voort uit het Europese ex-ante denken over persoonsgegevensbescherming, waarin verwerking van persoonsgegevens - simpel gezegd - alleen is toegestaan voor zover dat nodig is en de verantwoordelijke fatsoenlijk met de verzamelde informatie omspringt. Er valt echter, in het licht van de risico's van de glazen samenleving, ook veel te zeggen voor de Amerikaanse positie ten aanzien van privacybescherming, die gestoeld is op het idee dat onbelemmerd verzamelen en verwerken toelaatbaar is, zolang de schade die daardoor eventueel ontstaat maar door het slachtoffer verhaald kan worden.
Voor de naleving van de privacywet in een glazen samenleving ligt 'the best of both worlds' in een tussenpositie tussen de Amerikaanse en Europese benadering van privacybescherming, waarbij op voorhand privacygaranties worden ingebouwd en de normen vervolgens langs de lijnen van een krachtig toezicht worden gehandhaafd.
Daarnaast blijft uiteraard het stimuleren van privacybewustzijn van alle bij de glazen samenleving betrokkenen - burgers, bedrijfsleven én overheid - van belang. Als we afgaan op de recent hernieuwde, brede maatschappelijke belangstelling voor de milieuproblematiek dan zouden privacyvoorvechters wel eens gebaat kunnen zijn bij een internationale, door mediagenieke kopstukken gepropageerde campagne die burgers actief betrekt bij het vinden van een oplossing en overheden onder druk zet om actie te ondernemen. Zondag 28 januari 2008, de dag die door de Raad van Europa is uitgeroepen tot internationale privacydag, zou daarvoor bij uitstek de gelegenheid bieden.

Mr. J. Kohnstamm en dr. L. Dubbeld

NOTEN
1. [Terug]
Zie bijvoorbeeld David Lyon, Surveillance Studies: An Overview, Cambridge/Malden: Polity Press 2007.
2. [Terug]
Zie bijvoorbeeld David Murakami Wood (red.), A report on the surveillance society: for the Information Commissioner by the Surveillance Studies Network, september 2006.
3. [Terug]
Alan Travis, 'New powers vital to avert surveillance society, says watchdog', The Guardian 1 mei 2007, .
4. [Terug]
Vergelijk Bert-Jaap Koops en Merel Prinsen, 'Glazen woning, transparant lichaam: een toekomstblik op huisrecht en lichamelijke integriteit', NJB 2005, p. 624 (afl. 12).
5. [Terug]
Oscar Gandy, The panoptic sort: a political economy of personal information, Boulder: Westview 1993.
6. [Terug]
Susanne Lace (ed.), The glass consumer: life in a surveillance society, Bristol: Policy Press/National Consumer Council 2005.
7. [Terug]
Dit is niet alleen het geval voor de sectoren die wij hier bespreken, maar ook, zoals blijkt uit een eerder dit jaar gepubliceerd rapport van het Rathenau Instituut, op het gebied van opsporing en terrorismebestrijding. Zie Anton Vedder, Leo van der Wees, Bert-Jaap Koops &

Paul de Hert, Van privacyparadijs tot controlestaat? Misdaad- en terreurbestrijding in Nederland aan het begin van de 21ste eeuw, Den Haag: Rathenau Instituut 2007.
8. [Terug]
European Parliamentary Technology Assessment network (EPTA), Privacy and ICT in Europe: experiences from technology assessment of ICT and privacy in seven different European countries, 16 oktober 2006.
9. [Terug]
Zie Olga van Ditzhuijzen, 'Google als digitale detective: op web staan persoonlijke gegevens', NRC-Handelsblad 27 maart 2007.
10. [Terug]
Zie bijvoorbeeld European Parliamentary Technology Assessment network (EPTA), Privacy and ICT in Europe: experiences from technology assessment of ICT and privacy in seven different European countries, 16 oktober 2006.
11. [Terug]
Royal Academy of Engineering, Dilemmas of privacy and surveillance: challenges of technological change, maart 2007.
12. [Terug]
ISOC, 'ISOC.nl: volledig verbod op gebruik externe sitemonitoring bij overheid', 27 juni 2007, .
13. [Terug]
Zie Chip Walter, 'Privacy isn't dead, or at least it shouldn't be. A Q&A with Latanya Sweeney', Scientific American, 27 juni 2007, .

links

New powers vital to avert surveillance society, says watchdog, Alan Travis, The Guardian, 1 mei 2007
Glazen woning, transparant lichaam. Een toekomstblik op huisrecht en lichamelijke integriteit, dr B.J. Koops, mr M. Prinsen, NJB, aflevering 12 van 25 maart 2005
Privacy and ICT in Europe: experiences from technology assessment of ICT and privacy in seven different European countries, European Parliamentary Technology Assessment network (EPTA), 16 oktober 2006
Google als digitale detective: op web staan persoonlijke gegevens, Olga van Ditzhuijzen, NRC Handelsblad, 27 maart 2007
ISOC.nl: volledig verbod op gebruik externe sitemonitoring bij overheid, ISOC, 27 juni 2007
Privacy isn't dead, or at least it shouldn't be. A Q&A with Latanya Sweeney, Chip Walter, Scientific American, 27 juni 2007
Dilemmas of privacy and surveillance: challenges of technological change, William H. Dutton, Oxford Internet Institute, maart 2007