Rapport over de bewakingsstaat

Voor de Information Commissioner

Voor de Information Commissioner, door het Surveillance Studies Network

Samenvatting

september 2006

Geredigeerd door:

Kirstie Ball en David Murakami Wood

Materiaal geleverd door:

Louise Amoore
Kirstie Ball
Steve Graham
Nicola Green
David Lyon
David Murakami Wood
Clive Norris
Jason Pridmore
Charles Raab
Ann Rudinow Saetnan

Inleiding

In juni 2006 kreeg het Surveillance Studies Network van de Britse Information Commissioner de opdracht een rapport te schrijven over de bewakingsstaat. Dit document is een samenvatting van dat rapport. Het is verdeeld in drie hoofdstukken, die alle belangrijke punten uit het rapport omvatten. Het eerste hoofdstuk behandelt de bewakingsstaat inhoudelijk: welke definities worden gehanteerd, wat zijn de problemen en implicaties. Het tweede hoofdstuk gaat over het functioneren van de bewakingsstaat en het derde over enkele problemen waar de bewakingsstaat wet- en regelgevers voor stelt.

1. Bewakingsstaat: overzicht, achtergrond, definities

We leven in een bewakingsstaat. Het is zinloos om te spreken over de bewakingsstaat in de toekomende tijd. In alle rijke landen is bewaking een dagelijks verschijnsel, niet alleen overdag, maar ook 's nachts. Het gaat er niet alleen om dat bewakingscamera's ons doen en laten honderden keren per dag registreren of dat caissières in de supermarkt onze klantenkaarten willen controleren. Het gaat erom dat deze systemen een fundamentele, complexe infrastructuur vormen en dat er als vanzelfsprekend van wordt uitgegaan dat het verzamelen en verwerken van persoonsgegevens van vitaal belang is voor onze huidige samenleving.

Er zijn altijd bepaalde vormen van bewaking geweest: mensen houden elkaar in de gaten uit zorgzaamheid, uit voorzorg en om heimelijk informatie te vergaren. Zo'n 400 jaar geleden is men echter begonnen met het structureel toepassen van 'rationele' methoden die geleidelijk de plaats in hebben genomen van de informele, sociale netwerken en controles waarop het zakenleven en overheden zich vroeger verlieten. De gewone sociale banden van mensen werden als onbelangrijk ter zijde geschoven, zodat familiebanden en persoonlijke contacten het soepele functioneren van deze nieuwe, maatschappelijke structuren, de zogenaamde 'bureaucratieën', niet in de weg zouden staan. Maar het goede nieuws was dat burgers en uiteindelijk ook arbeiders op die manier konden verwachten dat hun rechten zouden worden gerespecteerd, omdat ze immers werden beschermd door een nauwgezette administratie en de wet. Bewakings- en controlesystemen tierden welig op basis van de onpersoonlijke, bureaucratische regelgeving. Na de oorlog werd de bureaucratie verder geperfectioneerd door de nieuwe informatietechnologie die de snelheid van gegevensverwerking, beheer en coördinatie sterk verbeterde. Met dit rapport willen wij deze ontwikkeling, die nog wordt versterkt door de verbeterde identificatie- en opsporingsmethoden van militaire diensten en politiediensten, onder de aandacht brengen. Bewaking neemt toe als onderdeel van de moderne samenleving.

Wat is er zo verkeerd aan een bewakingsstaat?

Wanneer we inzien dat bewaking een product is van de moderne samenleving, vermijden we twee valkuilen: bewaking beschouwen als een duivels plan van kwaadaardige machthebbers en denken dat bewaking een onvermijdelijk gevolg is van technologische vooruitgang (en natuurlijk zien de meest paranoïde personen de twee als één en dezelfde). Maar als we bewaking in het juiste perspectief plaatsen, wil dat nog niet zeggen dat er niets aan de hand is. Het betekent alleen dat we de oorzaken van de problemen zorgvuldig moeten bepalen en dat we waakzaam moeten blijven en de problemen onder de aandacht moeten brengen.

Bewaking heeft twee kanten en de voordelen ervan verdienen erkenning. Aan grootschalige systemen zijn tegelijk echter altijd risico's verbonden en we weten dat macht nu eenmaal corrumpeert of in elk geval bij degenen die macht uitoefenen leidt tot een verwrongen visie. Grootschalige, technologische infrastructuren leiden gemakkelijk tot grootschalige problemen. Eén onopzettelijke of onbezonnen toetsaanslag kan gemakkelijk desastreuze gevolgen hebben. Denk maar aan de vrijgave door AOL in augustus 2006 van twintig miljoen online zoekopdrachten van gewone gebruikers ten behoeve van

'onderzoeksdoeleinden'. Het bestand zou zijn ontdaan van alle identifiers, maar het was een fluitje van een cent om namen te koppelen aan de zoekbestanden.[1]

Zo moeten we ook rekening houden met corruptie en verkeerde inzichten van machthebbers. Nogmaals, we hoeven ons geen boosaardige tiran voor de geest te halen die de sleutels in hand krijgt om in te breken in bestanden van de sociale dienst of met medische gegevens om het probleem inzichtelijk te maken. Het soort corrumperende macht waar we op doelen, heeft ook betrekking op leiders die een of ander hoger doel aanroepen (zoals het winnen van een oorlog) om ongebruikelijke of uitzonderlijke maatregelen te nemen. In de VS werden Japanse Amerikanen tijdens de Tweede Wereldoorlog met behulp van – meestal illegale – bevolkingsgegevens geïnterneerd. Een meer recent voorbeeld is dat veel islamitische Amerikanen worden gebrandmerkt als 'reisgevaarlijk' door ze te plaatsen op 'no-fly' lijsten of ze anderszins te onderwerpen aan discriminerende maatregelen die in een andere context worden veroordeeld als overduidelijk onrechtvaardig.[2]

In de wereld van high-tech en globalisering van de handel zijn talloze voorbeelden te vinden van de onbedoelde gevolgen van goed bedoelde acties en maatregelen. Om concurrerend te blijven hanteert het bedrijfsleven kennelijk het adagium "Ken uw klanten" en stemmen bedrijven hun reclamecampagnes en zelfs de locatie van hun fabrieken en winkels daarop af. Niemand beweert dat de winkelchef die alleen de meest kredietwaardige klanten naar zijn winkel wil lokken, een scheve schaats rijdt als hij de kredietwaardigheidscontrole van Experian inroept. Op zoek naar grotere winstgevendheid is zo'n handelswijze alleszins begrijpelijk. Maar het resultaat – het onbedoelde gevolg – van het doorspitten van bestanden om een winstgevende klandizie te creëren is dat sommige groepen een speciale behandeling krijgen op basis van hun koopkracht en anderen hun heil elders moeten zoeken.[3]

De kern van de zaak is dat al die moderne bewakingsprocedures en –systemen een wereld scheppen die ervan uitgaat dat wij in wezen niet worden vertrouwd. Bewaking voedt argwaan.[4] De werkgever die zijn bedrijfscomputers voorziet van toetsaanslagbewaking of GPS-systemen installeert in bedrijfswagens, zegt in feite dat hij zijn werknemers niet vertrouwt. De sociale dienst die tandenborstels laat tellen of klikgedrag beloont op zoek naar bewijzen voor een gezamenlijke huishouding, zegt in feite dat zij de mensen niet vertrouwt. En dat geldt ook voor ouders die webcams en GPS-systemen inzetten om het doen en laten van hun tieners te controleren. Vaak gebeurt dit alleen maar uit (voor)zorg, zult u zeggen. Maar hoe ver mag dat gaan? Sociale relaties zijn gestoeld op vertrouwen en als we onszelf toestaan dat vertrouwen op dit soort manieren te ondermijnen plegen we op termijn sociale zelfmoord.

De definitie van bewaking; de bewakingsstaat nader omlijnd

In de bewakingsstaat is de maatschappelijke orde gestoeld op het gebruik van bewakingstechnieken. Onder bewaking staan houdt in dat bewakingssystemen namens de diensten en overheden die onze maatschappij structureren, informatie verzamelen en registreren over het doen en laten van mensen. Deze informatie wordt vervolgens gesorteerd, opgeschoond en gecategoriseerd en gebruikt als basis voor beslissingen die onze kansen in het leven beïnvloeden. Dit zijn bijvoorbeeld beslissingen over onze uitkeringsgerechtigdheid, onze positie op de arbeidsmarkt, onze toegang tot producten en diensten en ons recht op rechtsbescherming, over onze gezondheid, ons welzijn en onze vrijheden in

---

[1] Zie: Barbaro, A. en Zeller, T. 'A face is exposed for AOL searcher no. 4417749', *New York Times*, 9 August 2006. http://select.nytimes.com/gst/abstract.html?res=F10612FC345B0C7A8CDDA10894DE404482/

[2] Zie: Amnesty International USA (2004) *Threat and Humiliation: Racial Profiling, Domestic Security and Human Rights in the USA*, New York: Amnesty International USA, http://www.amnestyusa.org/racial_profiling/report/rp_report.pdf

[3] Lace, S (2005) *The Glass Consumer*, Bristol UK: Policy Press; Danna, A. and Gandy, O. (2002) 'All that glitters is not gold: Digging beneath the surface of data-mining' *Journal of Business Ethics*, 40: 373-386; Lyon, D. (ed.) (2003) *Surveillance as Social Sorting: Privacy, Risk and Digital Discrimination*, London and New York: Routledge.

[4] Besproken in: Lyon, D. (2003) *Surveillance after September 11*, Cambridge UK: Polity Press, 45-48, 142ff.

de publieke en private sfeer. In het dagelijks leven worden we met allerlei vormen van bewaking geconfronteerd, zoals:

- Videocamera's die onze gangen registreren – in gebouwen, winkelstraten, op autowegen en in woonwijken. Automatische systemen die nummerborden herkennen (en vaak ook gezichten).
- Elektronische tags om te controleren dat veroordeelden zich in hun proeftijd houden aan de regels voor reclassering; arrestanten die door de politie worden onderworpen aan DNA-onderzoek, waarvan de resultaten worden bewaard, of ze schuldig zijn of niet. 'Neigingen tot crimineel gedrag' worden in een steeds vroegere levensfase vastgesteld.
- We worden voortdurend gevraagd ons te legitimeren, voor uitkeringen, in de gezondheidszorg, etc. De Britse overheid wil nu een nieuw systeem van biometrische identiteitsbewijzen invoeren, waarbij 'biometrische gegevens' (vingerafdrukken en irisscans) worden gekoppeld aan een gigantische databank met persoonsgegevens.
- Als we op reis gaan naar het buitenland, wordt gecontroleerd wie we zijn, waar we naartoe gaan en wat we bij ons hebben en die informatie wordt opgeslagen. Onze paspoorten worden anders, voorzien van chips met informatie; er zijn nu ook voorstellen om niet alleen biometrische identiteitskaarten, maar ook biometrische paspoorten in te voeren.
- Veel scholen gebruiken smartcards en zelfs biometrische technologie om de gangen van kinderen na te gaan, te controleren wat ze eten en welke boeken ze van de bibliotheek lenen.
- Ons koopgedrag wordt geanalyseerd door software en de gegevens worden doorverkocht aan allerlei bedrijven. Als we service centers bellen of leningen, verzekeringen of hypotheken aanvragen, is wat we verdienen, waar we wonen en wie we zijn bepalend voor de snelheid waarmee we worden geholpen en wat ons wordt geboden.
- Onze telefoons, onze emailcommunicatie en ons internetgebruik kunnen worden afgetapt en gescreend op sleutelwoorden en ideeën door de Britse en Amerikaanse inlichtingendiensten.
- De bedrijven waar we werken houden niet alleen ons functioneren en onze productiviteit, maar ook ons gedrag en onze levenstijl buiten werktijd steeds nauwlettender in de gaten.

Overal waar we worden geconfronteerd met doelbewuste, routinematige, systematische en doelgerichte aandacht voor onze persoonsgegevens, om deze te controleren of te beheren, om rechten of invloed uit te oefenen of om belangen te beschermen, is sprake van bewaking. Samengevat:

- De aandacht is *doelbewust* – de bewaking wordt gerechtvaardigd op grond van overwegingen van bestuur, gerechtigdheid of een ander overeengekomen, openbaar doel.
- Daarnaast is zij *routinematig* – bewaking is onderdeel van ons dagelijks leven.
- De bewaking wordt *systematisch* uitgevoerd volgens een vooropgezet patroon en is niet steekproefsgewijs.
- De bewaking is *doelgericht*. Bewaking heeft vaak betrekking op identificeerbare personen, van wie de gegevens worden verzameld, opgeslagen, overgebracht, opgehaald, vergeleken, geëxploiteerd en verhandeld.

Het kan gaan om allerlei soorten persoonsgegevens, zoals video-opnamen, biometrische gegevensbestanden (vingerafdrukken of irisscans) en content of, wat het meest voorkomt, numerieke of categorische gegevens. Omdat het vaak gaat om gegevens in de laatste categorie, die betrekking hebben op transacties, informatie-uitwisseling, statusinformatie, accounts, etc., heeft Roger Clarke dit aangeduid als 'dataveillance.'[5] Bij dataveillance (databewaking) worden de activiteiten of communicatie-uitingen van mensen bewaakt door middel van geautomatiseerde IT-systemen. Het is veel goedkoper dan directe of doelgerichte, elektronische bewaking en biedt daarom voordelen die vaak aanleiding vormen om het systeem uit te breiden, ook al zijn de gegevens niet strikt nodig voor het oorspronkelijke doel.

[5] Clarke, R. (2006[1997]) 'Introduction to dataveillance and information privacy', http://www.anu.edu.au/people/Roger.Clarke/DV/Intro.html#DV

De bewakingsstaat in perspectief 1: processen

We gaan nu de processen en problemen inventariseren die verbonden zijn aan de bovengeschetste bewakingsstaat. De bedoeling is te komen tot een overzicht of checklist van belangrijke punten van overweging in de discussie over de bewakingsstaat. Hoewel zij afhankelijk van tijd en plaats verschillen, hebben al deze punten gemeen dat ze van essentieel belang zijn om inzicht te krijgen in de basiselementen van de bewakingsstaat.

Het indelen in klassen of groepen is inherent aan de bewakingsstaat. Door de overheid en het bedrijfsleven worden grote databases met persoonsgegevens geanalyseerd en gecategoriseerd om doelmarkten en risicogroepen in kaart te brengen.[6] Wanneer men eenmaal in een hokje is geplaatst, komt men daar moeilijk uit. Sinds 9/11 heeft deze rubricering de vliegveiligheid mogelijk bevorderd (dat zullen we nooit weten), maar het heeft in elk geval geleid tot een ruwe indeling van groepen, met name van Moslims, met veel ongemak, ontberingen en zelfs martelingen als gevolg. Het indelen in groepen is in toenemende mate typerend voor de observatiemaatschappij/ controlestaat. Het geeft verschillende groepen verschillende mogelijkheden en leidt vaak tot subtiele, soms onbedoelde manieren om de maatschappij te structureren en beleidsmaatregelen te nemen zonder democratisch overleg.

Gegevensstroom: de door bewakingssystemen verzamelde gegevens stromen vrijelijk tussen computernetwerken. Veel mensen hebben in een bepaalde context geen bezwaar tegen het verstrekken van gegevens, maar wat als deze gegevens vervolgens worden overgebracht naar een andere context? Om kinderen te beschermen tegen mishandeling of fraude bij openbare diensten te bestrijden wordt vaak een beroep gedaan op steeds uitgebreidere databanken. Maar tegelijk is het zo dat het grote publiek en zelfs de gegevens uitwisselende diensten maar weinig weten over de weg die deze gegevens precies afleggen. Het idee heeft postgevat dat de overheid uit het oogpunt van veiligheid inlichtingen nodig heeft. In combinatie met de bestaande netwerkstructuur voor het matchen van databasegegevens heeft dit geleid tot een situatie waarin bewaking als het ware een eigen leven is gaan leiden en zijn eigen regels volgt. Die regels dienen in twijfel te worden getrokken, te worden onderzocht en gecontroleerd, vooral waar het processen betreft waarbij gegevens van de ene context in de andere worden geplaatst.

Van *functieverschuiving* is sprake, wanneer persoonsgegevens die voor een bepaald doel en voor een bepaalde functie worden verzameld en gebruikt, migreren naar andere omgevingen waarin sprake is van nog intensievere bewaking en verdergaande inbreuken op de privacy. Omgevingen waarin het oorspronkelijke doel van de informatie-inwinning dus met voeten wordt getreden, maar die niettemin maatschappelijk, ethisch en wettelijk aanvaardbaar worden geacht. In het geval van de Oyster cards in het Verenigd Koninkrijk (OV-kaarten) werden gegevens die relevant waren binnen het kader van het openbare vervoer, in toenemende mate gebruikt als bron van inlichtingen voor de politie.[7] Functieverschuiving vindt meestal ongemerkt plaats, als onderdeel van een administratieve verbetering. Omdat door de voortschrijdende technologie steeds grotere hoeveelheden informatie kunnen worden uitgewisseld en organisatorische efficiency vaak wordt aangemerkt als een zaak van de hoogste prioriteit, worden de consequenties van functieverschuiving voor de burger echter maar al te vaak verdoezeld, genegeerd of gebagatelliseerd.

Technologie: Technologie is van essentieel belang voor bewaking, maar hierbij moeten wel twee belangrijke punten worden onderscheiden: In de eerste plaats komen directe, niet op technologie gestoelde vormen van 'persoonsbewaking' nog steeds voor, vaak gekoppeld aan vormen van bewaking met een meer technologisch karakter. In de tweede plaats is de oorzaak of de omvang van de tegenwoordige bewakingsactiviteiten niet te wijten aan de technologie. De mogelijkheden van een nieuw systeem kunnen niet van tevoren worden getaxeerd op de eventuele consequenties in termen

[6] Zie het klassieke onderzoek van: Gandy, O. (1993) *The Panoptic Sort: A Political Economy of Personal Information*, Boulder CO: Westview Press.
[7] Zie: 'Oyster data use rises in crime clamp-down' *The Guardian*, 13 March 2006, http://politics.guardian.co.uk/foi/story/0,,1730771,00.html

van bewaking. Voor een juist inzicht in de bewakingsproblematiek moeten we begrijpen hoe de technologie werkt, hoe technologie wordt gebruikt (dit is een interactief proces, waarbij zowel interne medewerkers als IT-consulenten en IT-werkers betrokken zijn) en hoe technologie de werking van een organisatie beïnvloedt. Bovendien hebben we voldoende inzicht in deze materie nodig om de politiek en de praktijk te kunnen beïnvloeden, zoals we bij onze latere bespreking van de mogelijke gevolgen willen aantonen.

Een vaak gehoord (onterecht, zoals we later zullen zien) argument van voorstanders van technologie is dat technologie de bezorgdheid over de bewakingsstaat juist goeddeels kan wegnemen. Er zijn inderdaad zogenaamde Privacy Enhancing Technologies (PET's) die de groei van technologische bewaking kunnen intomen en het gebruik daarvan dient waar nodig te worden bevorderd. Maar deze PET's bieden op zijn best slechts een gedeeltelijke oplossing. We zijn terecht op ons hoede voor het bestrijden van technische problemen met technische oplossingen. Zoals we zullen zien, is de praktijk van de bewakingsstaat veel te complex voor dergelijke oppervlakkige oplossingen.

De bewakingsstaat in perspectief 2: problemen

Privacy, ethiek, mensenrechten: Sinds de jaren zeventig is er veel nagedacht en gesproken over het wettelijke kader van bewaking, wat in Europa heeft geleid tot wetgeving op het gebied van de bescherming van persoonsgegevens en in andere landen op het gebied van privacy. Dergelijke wetgeving is gebaseerd op een bepaalde opvatting over privacy. Hoewel de zogenaamde 'Fair Information Principles' (FIPs)[8] zijn ontwikkeld, blijken beleidsmakers moeilijk te doordringen van het belang van de *maatschappelijke* implicaties van privacy[9] laat staan van de noodzaak problemen aan te pakken die te maken hebben met de bewakingsstaat als zodanig. De bewakingsstaat stelt ons voor vraagstukken op het gebied van ethiek en de rechten van de mens die het domein van de privacy overstijgen. Men moet er bijvoorbeeld niet van uitgaan dat mensen die aan bewaking worden onderworpen, zichzelf maar moeten beschermen. Het gaat bijvoorbeeld om de volgende drie belangrijke kwesties:

Sociale uitsluiting, discriminatie: Bewaking varieert in intensiteit, zowel geografisch als wat betreft sociale klasse, etnische achtergrond en sekse. Bij bewaking, inbreuk op de privacy en bescherming van de privacy wordt onderscheid gemaakt tussen groepen en worden sommigen bevoordeeld en anderen daardoor dus benadeeld. De verzorgingsstaat, eens het paradepaardje van sociaal-democratische regeringen, is verschrompeld tot risicobeheer en om de risico's van een situatie te beheren is volledige kennis van die situatie nodig. Zie daar de link met de bewakingsstaat. Dus worden persoonsgegevens verzameld om te weten waar middelen moeten worden ingezet.[10]

*Keuze, macht en delegeren van macht***:** Gewone mensen kunnen een verschil maken en doen dat ook, vooral wanneer zij erop staan dat regels en wetten in acht worden genomen, het systeem aan de kaak stellen of weigeren toe te staan dat hun gegevens worden gebruikt voor doelen waar ze het fijne niet van weten of waarover ze twijfels hebben. Maar hebben individuen en groepen ook invloed op de mate van de bewaking en controle waaraan ze worden blootgesteld en in hoeverre kunnen ze het verzamelen en het gebruik van persoonsgegevens beperken? Als het bewakingssysteem onderdeel uitmaakt van de infrastructuur en als de werking ervan versluierd wordt door technische mystificaties, is het inderdaad bijzonder moeilijk om nog enig verschil te maken. Pas wanneer er bijvoorbeeld een schandaal ontstaat rond identiteitsdiefstal, zullen consumenten zich bewust worden van de mate van profielanalyse die grote bedrijven verrichten.[11] Ook in dat geval zal in eerste instantie de noodzaak van beveiliging worden benadrukt – hoe kan soortgelijke fraude worden voorkomen – en zal pas in laatste instantie worden gedacht aan het beteugelen van de macht van bedrijven en overheidsdiensten om zo veel

[8] FIP's zijn het Amerikaanse equivalent van de Europese 'principes van gegevensbescherming.'
[9] Zie de uitstekende verhandeling over het maatschappelijk belang van privacy in: Regan, P. (1005) *Legislating Privacy: Technology, Social Values, and Public Policy*, Chapel Hill: University of North Carolina Press.
[10] Ericson, R. and Haggerty, K. (1997) *Policing the Risk Society*, Toronto: University of Toronto Press.
[11] Zie het hoofdartikel de *New York Times*, 'The data-fleecing of America', van 21 juni 2005.

gegevens zonder aanzien des persoons te verwerken. Het individu is ernstig in het nadeel waar het gaat om het beheersen van de effecten van bewaking.

Transparantie, verantwoordingsplicht: Individuen en groepen vinden het moeilijk om te achterhalen wat er met hun persoonsgegevens gebeurt, wie die gegevens verwerkt, wanneer dit gebeurt en voor welk doel. Stap voor stap worden hun persoonsgegevens echter gebruikt om hun levenskansen en keuzes te bepalen. Gezien de macht van grote organisaties die beschikken over geavanceerde bewakingsfaciliteiten is het echter niet meer dan billijk wanneer de gewone man een vinger in de pap heeft, al is het maar uit principe. Hieraan kan worden gewerkt, niet alleen door gespecialiseerde diensten, maar ook door belangengroepen en de massamedia.

Organisaties dienen hun verantwoordingsplicht na te komen, vooral waar geavanceerde bewaking routinematig wordt toegepast, met mogelijk schadelijke gevolgen. Hoewel er diverse saillante voorbeelden zijn van slechte bewakingspraktijken op de werkplek, zijn vakbonden er in een aantal gevallen in geslaagd werkgevers te dwingen hun buitensporige bewakingsdrift in te tomen. Wanneer werkgevers op transparante wijze zouden uitleggen wat hun bewaking behelst en met hun werknemers om de tafel zouden zitten om toestemming te krijgen, zou dit overigens veel misverstanden kunnen wegnemen. Wat betreft de bewaking van consumenten zijn er echter geen analoge voorbeelden te vinden, terwijl winkelketens als Tesco en Walmart toch beschikken over een vrijwel ongekende datamacht. De opkomst van de bewakingsstaat vereist dat we de aandacht verleggen van onze individuele verantwoordelijkheid om onze privacy te beschermen naar de verantwoordingsplicht van grote gegevensverwerkers. De inspanning die dit vergt, is te vergelijken met de inspanningen van regelgevers om controlemaatregelen op te leggen en bewakingspraktijken aan banden te leggen.

2. Onderzoek naar de bewakingsstaat

Het Surveillance Studies Network heeft opdracht gegeven tot het maken van een aantal deskundigenrapporten waarin de volgende onderwerpen aan de orde komen: Gezondheidszorg, de consument, werkgelegenheid, overheidsdiensten, burgerrechten, criminaliteit en rechtspraak, communicatie, gebouwde omgeving en infrastructuur en grenzen. Uit deze rapporten zijn diverse kernthema's te distilleren, die in vier groepen kunnen worden verdeeld: de context van de bewakingsstaat, bewakingstechnologie, de werking en implementatie van bewakingssystemen en ten slotte de gevolgen van bewaking voor individuen en groepen in de samenleving. Tussen deze aandachtsgebieden bestaat natuurlijk veel overlap, zoals er ook nog veel onderwerpen zijn die in dit bestek niet aan de orde kunnen komen.

De context van de bewakingsstaat

Eerst zullen we diverse onderliggende trends in onze westerse maatschappij noemen die ten grondslag liggen aan de bewakingsstaat. Die trends betreffen: risico en veiligheid, de militarisering van bewaking, de economie van bewaking en ten slotte de groeiende persoonsgegevensindustrie.

Risico en veiligheid: We leven in een samenleving waarin risico een obsessie is. Risicobeheertechnieken om externe en interne bedreigingen het hoofd te bieden vormen tegenwoordig een essentieel onderdeel van organisatorische activiteiten. Een *preëmptieve* in plaats van een *preventieve* benadering van risico doet tegenwoordig opgeld.[12] Zo is door het gebruik van gegevenszoeksystemen en profileringsmethoden om risico's in kaart te brengen het accent verschoven naar het screenen van het gedrag en de transacties van het grote publiek.[13] Deze screening kan vervolgens worden gebruikt om maatregelen te richten op individuen of groepen die een verhoogd

[12] Ewald, F. (2002) 'The return of Descartes' malicious demon: an outline of a philosophy of precaution', in Baker, T. and Simon, J. (eds.), *Embracing Risk: The Changing Culture of Insurance and Responsibility*, Chicago: University of Chicago Press.

[13] Valverde, M. en Mopas, M. (2004) 'Insecurity and the Dream of Targeted Governance', in Larner, W. en Walters, W. (eds.) *Global Governmentality: Governing International Spaces*, London: Routledge.

risico zouden lopen of een verhoogd risico zouden vormen voor anderen. Het verzamelen en analyseren van informatie, met inbegrip van gegevens over identificeerbare personen, is van vitaal belang. Dit kan persoonlijke en maatschappelijke voordelen opleveren, maar tegelijk heeft deze opvatting van veiligheid en beveiliging belangrijke implicaties op het gebied van vrijheid, privacy en andere maatschappelijke waarden, evenals op het gebied van innovatie en verandering.

Diverse voorbeelden illustreren deze trend van risicobeoordeling en een preëmptieve aanpak:

- Epidemiologie en de toepassing van modellen op het gebied van medische bewaking[14] om individuele gevallen in kaart te brengen, gevallen te registreren voor statistische analyse en bevolkingsgroepen te identificeren die gevaar lopen in verband met bepaalde ziekten
- Risicoanalyse van personen, gezinnen en buurten in het kader van kinderbescherming, geestelijke gezondheidszorg en strafrecht
- De risico's die reizigers vormen voor de nationale veiligheid in kaart brengen op basis van passagierslijsten en financiële transacties
- De relatieve waarde van individuele klanten en hun geodemografische profielen evalueren

De militarisering van bewaking: Militaire bewaking is een van de weinige gebieden waarop inderdaad sprake is van globalisering. De aarde wordt omgeven door tientallen militaire bewakingssatellieten en transnationale communicatiesystemen worden grondig geïnfiltreerd door militaire bewakingssystemen. Twee moderne voorbeelden van technologieën die zijn ontworpen met ingebouwde militaire functies zijn het Global Positioning System en het internet. De geschiedenis van de moderne bewakingssystemen is echter terug te voeren op de Command Communications, Control en Intelligence (C3I) systemen in de Tweede Wereldoorlog en de Koude Oorlog, bedoeld om van de aarde een compleet verdedigbare en veilige ruimte te maken.[15] De tweeledige functie van GPS en het internet blijkt niet alleen uit de toepassing ervan voor overheidsdoelen, maar ook uit de toenemende militarisering van het taalgebruik waar het de veiligheid betreft: staatsmedia en massamedia hebben het over 'threat assessment', de 'war on drugs' en de 'war on crime', de 'oorlog tegen het terrorisme', harde rechtsmaatregelen, 'zero tolerance', etcetera. 'Elektronische oorlogvoering' is het duistere domein van geheime, militaire operaties ontstegen en tegenwoordig gemeengoed in het bedrijfsleven, waar bedrijfsspionage behoort tot de praktijk van alledag en specialisten op het gebied van computerpenetratie en beveiliging worden aangeduid als 'knowledge warriors'. Veel bedrijven die zijn gespecialiseerd in bewakingstechnologie onderhouden nauwe banden met het militaire apparaat, maar verkopen ook aan niet-militaire gebruikers. TRW, bijvoorbeeld, een belangrijke leverancier van het Amerikaanse Ministerie van Defensie, werd een van de marktleiders op het gebied van biometrische systemen voor niet-militaire doelen. Het Franse bedrijf Sagem produceert alles, van mobiele telefoons tot en met bewakingssoftware en onbemande luchtverkenningssystemen.

De beveiligingssector: Deze nieuwe bedrijven maken samen met de traditionele beveiligingsleveranciers en de grote militaire leveranciers deel uit van de zogenaamde 'beveiligingsindustrie'. Andere industriële sectoren, zoals de telecommunicatie-industrie, de computerindustrie en het bank- en verzekeringswezen, dragen ook in belangrijke mate bij tot de groei op het gebied van bewaking. De beveiligingsindustrie is de afgelopen jaren gegroeid als kool. Volgens de top-100 index van het Amerikaanse adviesbureau Security Stock Watch[16] hebben de groeicijfers van de industrie als geheel de indexcijfers van de Dow Jones en de high-tech NASDAQ beurs steeds

[14] Zie over de dominante rol van de gezondheidssector en de medische wetenschap, waar medische technologie vaak wordt beoordeeld met behulp van aan de epidemiologie ontleende methoden en resultaten, onder andere: Ashmore, M., Mulkay, M.J. en Pinch, T.J. (1989) *Health and Efficiency: A Sociology of Health Economics*, Buckingham: Open University Press.

[15] de Landa, M. (1991) War in the Age of Intelligent Machines, Cambridge MA: MIT Press; Edwards, P. (1997) Computers and the Politics of Discourse in Cold War America, Cambridge MA: MIT Press.

[16] Deze index omvat 'biodefensie', 'milieubeveiliging', 'fraudepreventie', 'militaire defensie', telecommunicatie netwerkbeveiliging' en 'fysieke beveiliging' (schermen, videobewaking, etc.).

weer overtroffen[17]. Aan het eind van het boekjaar 2005-2006 was de index in drie jaar tijd meer dan verdubbeld en vertegenwoordigden de top-100 bedrijven van de index een marktwaarde aan aandelenkapitaal van meer dan 400 miljard dollar.

Persoonsgegevensindustrie: Bewaking is niet uitsluitend het domein van landen en bedrijven – ook gewone burgers maken ervan gebruik. Na de bomaanslagen in Londen in 2005 raadden zowel tv-bedrijven als de politie de mensen aan om met hun mobiele telefooncamera's foto's te nemen van verdachte personen. Steeds meer mensen, vooral kinderen en jongeren, laten anderen meegenieten van hun doen en laten en volgen de wederwaardigheden van anderen via online webcams[18] en sociale netwerksites als *MySpace* en *Bebo*. Ook zijn er mensen die toegang weten te vinden tot kennisbanken en hun 'datadubbelganger' in bijvoorbeeld de databases van kredietwaardigheidsbedrijven als *Experian* en *Equifax* op die manier kunnen beheren. Deze kredietbewakers bieden burgers online toegang tot hun kredietgegevens, zodat ze misleidende informatie kunnen aanvechten en corrigeren. Deze combinatie van vrijwillige transparantie van bedrijven en de autodidactische kennis van personen kan niet worden gekenmerkt als een vorm van regulering, ondanks het feit dat er een nieuwe generatie burgers opgroeit die gewend is zowel gebruiker als voorwerp van bewaking te zijn.

Bewakingstechnologie

Hoewel we het belang van niet-technologische bewaking niet moeten vergeten (zoals afluisteren, spioneren en klikken), is dit hoofdstuk gewijd aan zaken die verband houden met bewakingstechnologie. Eerst behandelen we de overlappende progressie op vier gebieden: telecommunicatie, videobewaking, databases, biometrische toepassingen en systemen op het gebied van lokalisering, tagging en tracering. Daarna bespreken we het onderlinge verband tussen verschillende technologieën en de tendens dat bewakingstechnologie tegelijkertijd verdwijnt en zich overal verspreidt. Tot besluit bespreken we de grenzen van de technologische ontwikkeling.

Technologische ontwikkeling: Het valt niet te ontkennen dat bewaking door de nieuwe technologie wezenlijk is veranderd. De huidige technologische bewakingssystemen kennen geen inherent 'goed' of 'kwaad'. Efficiënte nationale databases kunnen zowel worden gebruikt om de beoogde kwaliteit gezondheidszorg te leveren als voor het uitschakelen van politieke tegenstanders. Maar het gaat er niet alleen om hoe ze worden gebruikt. Alle systemen zijn ontwikkeld binnen bepaalde organisaties die bepaalde doelen en belangen hebben. Hier gaan we nader in op bepaalde technologieën en wat ze vermogen.

Telecommunicatie: Bewaking in de telecommunicatie heeft te maken met de mate waarin personen, organisaties en bedrijven informatie over het gebruik en de inhoud van telecommunicatie kunnen bewaken, sorteren en opslaan, zowel tussen systemen onderling als tussen mensen en systemen. Sinds de staat telefoons ging aftappen, heeft de technologische vooruitgang allerlei verschillende systemen in het leven geroepen voor telecommunicatiedoeleinden en de mogelijkheden van bewaking sterk uitgebreid. De locatie van een mobiele telefoon kan bijvoorbeeld gemakkelijk worden bepaald door op het signaal van het apparaat en de ontvangst daarvan door diverse ontvangststations die signalen uitwisselen, een driehoeksmeting te verrichten – deze informatie kan vervolgens worden opgeslagen voor later onderzoek. Het zogenaamde 'ECHELON'-systeem – het wereldwijde aftapnetwerk van de Amerikaanse veiligheidsdienst NSA – heeft een gigantisch basisstation in Menwith Hill, North Yorkshire, dat automatisch en routinematig alle telecommunicatie in en uit het Verenigd Koninkrijk filtert op sleutelwoorden en zinnen en steeds verfijndere toepassingen gebruikt op het gebied van spraakherkenning en zelfs betekenisherkenning[19].

---

[17] *SecurityStockWatch.com 100 Index*, augustus 2006, http://www.securitystockwatch.com/

[18] Koskela, H. (2004) 'Webcams, TV Shows and Mobile phones: Empowering Exhibitionism', *Surveillance & Society*, CCTV Special (eds. Norris, McCahill en Wood), 2(2/3): 199-215, http://www.surveillance-and-society.org/cctv.htm

[19] Campbell, D. (1999) Development of Surveillance Technology and Risk of Abuse of Economic Information (An appraisal of technologies of political control) Volume 2/5: Interception Capabilities 2000, Luxembourg:

Videobewaking: Fotografische bewaking bestaat al sinds het eind van de 19de eeuw. Volgens een uitgebreid onderzoek naar de installatie van CCTV camera's, dat begin jaren negentig werd gehouden naar aanleiding van pogingen de criminalisering van winkelgebieden in stadscentra tegen te gaan en uit angst voor terrorisme, zouden er in het Verenigd Koninkrijk nu zo'n 4,2 miljoen CCTV camera's zijn geïnstalleerd: één op elke 14 burgers,[20] en elke burger kan dagelijks door meer dan 300 camera's worden vastgelegd.[21] In de jaren negentig besteedde het Ministerie van Binnenlandse Zaken 78% van het budget voor misdaadbestrijding aan het installeren van CCTV-systemen[22] en het afgelopen decennium is naar schatting 500 miljoen pond aan overheidsgelden geïnvesteerd in de CCTV-infrastructuur.[23] Een onderzoeksrapport van het Ministerie van Binnenlandse Zaken concludeerde echter dat 'de onderzochte CCTV-systemen weinig effect hebben gehad op de algehele misdaadcijfers'.[24] Door de digitalisering is het automatische gebruik van CCTV-systemen verder toegenomen. Tot nu toe is dit vooral op het verkeer toegepast. Nummerborden worden gebruikt om de geregistreerde eigenaar te achterhalen. Handhaving van snelheidslimieten door middel van camerabewaking is in het Verenigd Koninkrijk toegenomen van zo'n 300.000 installaties in 1996 tot meer dan 2 miljoen in 2004, met een gemiddelde boete-opbrengst per jaar van zo'n 113 miljoen pond.[25] Deze ongebreidelde groei van staatstoezicht is in de pers steeds negatief ontvangen,[26] ondanks het feit dat snelheidscamera's, in tegenstelling tot open CCTV-systemen op straat, hebben geleid tot een aanzienlijke verlaging van het aantal doden en gewonden als gevolg van verkeersongelukken.[27] Er staan plannen op stapel om de capaciteit van het National Automatic Number Plate Recognition (ANPR) centre uit te breiden van 35 miljoen registraties per dag tot 50 miljoen per dag in 2008.

De Database: Allerlei gegevens kunnen nu veel sneller en nauwkeuriger worden verzameld, geclassificeerd en van kruisverwijzingen worden voorzien dan het geval was bij de papieren dossiers waar de moderne bureaucratie vroeger in grossierde. Bewaking waarbij gebruik wordt gemaakt van een database, kan gemakshalve worden aangeduid met 'dataveillance' ('datatoezicht'). Databases gekoppeld aan andere bewakingssystemen maken het ook mogelijk bewakingssoftware te gebruiken die de opnames of data bewerkt en vergelijkt met de databasegegevens. De toepassing van biometrische metingen is hierop gebaseerd. Dataveillance wordt op grote schaal toegepast in de marketing, de medische sector, voor opsporingsdoeleinden en grensbewaking.

In de *marketing* zijn de kosten van databasediensten betaalbaarder geworden, zodat veel bedrijven in de particuliere sector nu zo veel mogelijk gegevens verzamelen over hun klanten om hun marketingcommunicatie daar nauwkeuriger op af te stemmen. Gegevens over transacties (het gebruik van creditcards, transacties via mobiele telefoons, etc.), waarbij de identiteit van de zender is te achterhalen, worden gekoppeld aan aanvullende gegevens uit/van/over klantenkaartsystemen, klantenonderzoek, doelgroepen, prijsvragen, verzoeken om productinformatie, contacten met

---

European Parliament, Directorate General for Research, Directorate A, The STOA Programme; Wood, D (2001) The Hidden Geography of Transnational Surveillance, Unpublished PhD Thesis, University of Newcastle, UK.

[20] McCahill, M. and Norris, C. (2003), 'Estimating the extent, sophistication and legality of CCTV in London', in M. Gill (ed.) *CCTV*, Perpetuity Press.

[21] Norris, C en Armstrong, G. (1999), The Maximum Surveillance Society:The Rise of Closed Circuit Television, Oxford: Berg.:42

[22] ibid.: 54

[23] Norris, C. (2006) 'Closed Circuit Television: a review of its development and its implications for privacy', rapport opgesteld voor de driemaandelijkse vergadering van de Department of Homeland Security Data Privacy and Integrity Advisory Committee, 7 juni, San Francisco CA.

[24] Gill, M. and Spriggs, A. (2005). *Assessing the impact of CCTV*. London, Home Office Research, Development and Statistics Directorate, 43, 60-61.

[25] Wilkins, G. en Additcott, C. (1998) *Motoring Offences England and Wales 1996*, Home Office Statistical Bulletin, London: Home Office; Ransford, F., Perry, D. Murray, L. (2005) *Motoring Offences and Breath Test Statistics: England and Wales 2003*, Home Office Statistical Bulletin, London: Home Office.

[26] McCahill en Norris, 2003 *op cit*. n.44.

[27] PA Consulting (2004) *Denying Criminals the Use of the Road*, http://police.homeoffice.gov.uk/news-and-publications/publication/operational-policing/ANPR_10,000_Arrests.pdf?view=Binary

callcenters, website cookies, feedback forums voor consumenten en krediettransacties. Deze *interne* en vaak eigendomsrechtelijk beschermde gegevens worden vaak vergeleken met *externe* gegevens van overheidsdiensten (bijvoorbeeld het 'Centraal Bureau voor de Statistiek'), non-profit organisaties of in gegevensverzameling gespecialiseerde bedrijven. Via deze bronnen zijn postcodes gemakkelijk te achterhalen en de gevonden adressen worden vaak 'geprofileerd' met kenmerken als 'zuinige pensioentrekkers', 'nieuwkomers' of 'nette armoede'.[28] Eenvoudige matchingtechnieken en het gebruik van geodemografische profilering worden tegenwoordig versterkt door de meer geavanceerde, 'heuristische' (leer)processen van gegevensonderzoeksystemen, ook wel aangeduid als Knowledge Discovery in Databases (KDD). Op die manier worden binnen datasets ook tot dan toe onbekende, *niet voor de hand liggende* relaties ontdekt.[29] Het 'product' van deze systemen is wellicht het best zichtbaar als basis voor webpersonalisatiesystemen, zoals toegepast door Amazon.com, waarbij meerdere informatiebronnen worden gebruikt om de waarschijnlijke voorkeuren van de online shoppers te voorspellen.[30]

Biometrie: Alle nieuwe ID-systemen gebruiken een bepaalde vorm van biometrie: vingerafdrukken, irisscans, gezichtstopografie en hand-scans worden alle gebruikt op verschillende paspoort- en identiteitskaartsystemen. Wat biometrie zo aantrekkelijk maakt, is dat het menselijk lichaam een 'anker' bevat waaraan identiteitsgegevens kunnen worden gekoppeld. Deze biometrische identificator wordt de toegangspoort tot de opgeslagen informatie. Het gaat om deze convergentie van data mining en integratie met biometrische identificators. De verwachting is dat de nauwkeurigheid van identificatie toeneemt en fraude afneemt. Pincodes en wachtwoorden kan men vergeten of kwijtraken, maar het lichaam legt een vaste, directe koppeling tussen gegevensopslag en de identiteit van de persoon. De 'Oorlog tegen het terrorisme' heeft een vloedgolf van investeringen in biometrisch onderzoek en de toepassing van biometrie veroorzaakt. Sinds 9/11 werden biometrische technieken die in de VS al commercieel werden toegepast of daarvoor in aanmerking kwamen, snel opgespoord en gepresenteerd als de sleutel tot het winnen van dit nieuwe type oorlog.[31] Met de Patriot Act, die een impact heeft tot ver buiten de landsgrenzen van de VS, werd een wettelijk kader geschapen dat het mogelijk maakt biometrie vrijwel onbeperkt toe te passen voor de opsporing en herkenning van terroristische activiteiten. In het Verenigd Koninkrijk heeft de bovengenoemde vlucht van digitale CCTV geleid tot verder onderzoek naar de praktische mogelijkheden van biometrische CCTV-systemen en gezichtsherkenning op basis van eerdere experimenten in Newham, Birmingham en op andere locaties.

Lokalisering, tracering en tagging: Bewakingsactiviteiten worden steeds vaker herkend, opgezet en opgespoord met behulp van Geographical Information Systems (GIS's)[32]. De geografische bewegingen van mensen, voertuigen of goederen worden vaak getraceerd met behulp van RFID chips, Global Positioning Systems (GPS), smart ID cards, transponders of de radiosignalen van mobiele telefoons of draagbare pc's. Deze technologie wordt soms ook al toegepast bij de rechtshandhaving, bij grensbewaking en op de werkplek.

---

[28] De eerste categorie is afkomstig van het ACORN classificatiesysteem van het bedrijf CACI, en de twee laatste categorieën zijn MOSAIC classificaties van Experian. Meer informatie over deze producten is te vinden op http://www.caci.co.uk/acorn/ en http://www.business-strategies.co.uk/Content.asp?ArticleID=629. Zie ook: Burrows, R. en Gane, N. (binnenkort verkrijgbaar) 'Geodemographics, software and class.' *Sociology.*

[29] Meer informatie over de verschillen tussen KDD en data-mining is te vinden in Tavani, H.T. (1999) 'KDD, data mining, and the challenge for normative privacy.' *Ethics and Information Technology* 1: 265-273. Veel bronnen refereren aan data mining als het totale proces van gegevensverwerking voor de hier beschreven doelen. Zie Rygielski, C., Wang, J-C, en Yen, D.C. (2002) 'Data mining techniques for Customer Relationship Management.' *Technology in Society* 24: 483-502, Danna en Gandy (2002) *op cit.* n.6. Voor de duidelijkheid: de term KDD wordt hier gebruikt om het totale technische proces te definiëren dat bepaalde overeenkomsten (al dan niet voor de hand liggend) binnen datasets constateert en data mining als het verzamelen van belangrijke gegevens voor verdere gegevensanalyse.

[30] Fink, J., en Kosba, A. (2000) 'A review and analysis of commercial user modeling servers for personalization on the World Wide Web.' *User Modeling and User-Adapted Interaction* 10: 209-249.

[31] Amoore, L. (2006) 'Biometric borders: governing mobilities in the war on terror', *Political Geography* 25: 2: 336-351; Gates, K. (2005) 'Biometrics and post-9/11 technostalgia', *Social Text* 23(2): 35-53. Irma Van der Ploeg, 'Biometrics and the body as information', in Lyon, D. (ed.) (2003) *op cit*. n.3.

[32] Institute for the Future (2004) *Infrastructure for the New Geography*, Menlo Park, CA: IFTF.

Wat bijvoorbeeld de *rechtshandhaving* betreft, werden in mei 2004 631 volwassenen en 5751 jongeren, soms niet ouder dan twaalf, 'getagd', zodat ze hun berechting thuis konden afwachten in plaats van in bewaring te worden gehouden.[33] Ook uit de gevangenis ontslagen misdadigers worden onderworpen aan elektronische bewaking, als voorwaarde voor vervroegde vrijlating onder het Home Detention Curfew Scheme[34] of als voorwaarde voor voorwaardelijke vrijlating.[35] In de VS worden RFID smartcards getest bij de *bewaking van de grens* tussen de VS en Mexico. De RFID industrie prijst de mogelijkheden van deze technologie aan om gastarbeiders die de grens voor een beperkte periode passeren, te bewaken en te traceren. Na experimenten met dieren worden nu ook bij mensen RFID chips geïmplanteerd. In de VS zijn bij 70 mensen met degeneratieve hersenaandoeningen ook RFID chips geïmplanteerd, zodat ze gemakkelijker te traceren zijn[36] en er is één geval bekend waarbij een bedrijf bij twee werknemers chips heeft ingebracht in verband met toegangscontrole tot de *werkplek*.[37] De voortgaande ontwikkeling van de toepassing van real time geografische gegevens op consumentenprofielen creëert nog een gegevenslaag die bedrijven de mogelijkheid biedt hun marketingcampagnes af te stemmen op bepaalde consumenten. Dit zijn dus voorbeelden van technologieën waarbij het risico groot is dat de functie ervan zal 'verschuiven'.

Technologische synergie en functieverschuiving: Hoewel het belangrijk is te weten wat de functie is van afzonderlijke technologieën en systemen, speelt de synergie tussen technologieën of de convergentie van bewakingstechnologieën een steeds belangrijkere rol. Dit betreft een langetermijn trend binnen computersystemen en wordt ook gemotiveerd door de wens schaalvoordelen te creëren. Steeds meer systemen worden ontworpen uit het oogpunt van interoperabiliteit. Dit betekent ook dat nieuwe producten kunnen voortkomen uit oudere technologieën die op zichzelf door wetgevers werden begrepen en in een kader geplaatst, maar in combinatie een totaal onvoorziene, niet gereguleerde functie kunnen creëren. Bijvoorbeeld:

- Identiteitskaarten die verschillende doelen dienen – grenzen passeren, fraude bestrijden, toegang tot overheidsinformatie en eventueel ook commerciële (videoverhuur) en semi-commerciële (bibliotheken) doelen. Wanneer agenda's zoals de 'war on terror' die de migratie van ongewenste groepen aan banden legt, en ook de roep om oplossingen voor creditcardfraude de ontwikkeling van ID-systemen sturen, lijkt het 'onpersoonlijke' ethos van een klassieke bureaucratie enigszins te worden ondermijnd.
- ANPR in Londen werd oorspronkelijk ontwikkeld voor militaire doeleinden en geïnstalleerd om IRA plegers van bomaanslagen te identificeren, en wordt nu ingezet om het verkeer te regelen, de overheidskas te spekken en als beveiligingssysteem te dienen tegen een nieuwe generatie terroristen.

Naar een alomtegenwoordige bewakingsstaat: Technologieën egen het zwaarst, wanneer ze alomtegenwoordig zijn, als vanzelfsprekend worden beschouwd en grotendeels onzichtbaar zijn. De alomtegenwoordigheid van computersystemen (Ubicomp), ook wel aangeduid als 'ambient intelligence' (AmI), schept de voorwaarden voor alomtegenwoordige of algemeen verbreide bewaking door zowel in de fysieke als de virtuele omgeving te nestelen.[38] Elektronische diensten en domeinen

[33] NPS (National Probation Service) (2006) *Electronic Monitoring* 6. http://www.probation.homeoffice.gov.uk/output/Page137.asp#Current%20Programmes .

[34] Het Home Detention Curfew Scheme maakt het mogelijk veroordeelden tot een gevangenisstraf van drie maanden tot vier jaar twee weken tot vier en een halve maand eerder vrij te laten onder een avondklokregime dat door elektronische bewaking wordt gehandhaafd. In 2004/5 werden 19.096 veroordeelden onder deze regeling eerder vrijgelaten (*ibid*.: 6).

[35] NPS op cit.

[36] Het betreffende bedrijf is Verichip Corporation. http://www.verichipcorp.com/ .

[37] Waters, R. (2006) 'US group implants electronic tags in workers', *Financial Times*, 12 februari. http://www.ft.com/cms/s/ec414700-9bf4-11da-8baa-0000779e2340.html .

[38] Kang, R. en Cuff, D. (2005) 'Pervasive Computing: Embedding the Public Sphere,' *Washington and Lee Law Review* 62(1): 93-146. Cuff, D. (2002) Immanent domain: Pervasive computing and the public realm, *Journal of Architectural Education*, 57: 43-49.

zijn betrekkelijk gemakkelijk te beheren vergeleken met de straten in een stad, maar op veel drukke verkeerspunten in steden worden nu *zowel* elektronische *als* fysieke systemen gebruikt die nauw samenwerken. De combinatie van CCTV, biometrie, databases en opsporingstechnologie kan worden gezien als onderdeel van een veel breder onderzoek, vaak financieel gesteund uit het budget van de VS/VK voor de 'war on terror', naar het gebruik van gekoppelde 'intelligente' systemen om de bewegingen en het gedrag van miljoenen mensen, zowel in de tijd als in de ruimte, te bewaken. In de industrie wordt dit 'multiscale spatiotemporal tracking' genoemd.[39]

De grenzen van de technologie: De beloften van nieuwe technologie worden natuurlijk vrijwel nooit precies zo ingelost als oorspronkelijk verwacht. De verwachtingen over de biometrische technieken voor het USVISIT programma, bijvoorbeeld, werden om logistieke redenen van de geplande irisscans naar beneden bijgesteld tot digitale vingerafdrukken Er zijn ook problemen met de betrouwbaarheid,[40] 'failure to enrol (FTE)' (de biometrische informatie is onherkenbaar) en 'false non-match' (metingen komen niet overeen met de correct vastgelegde, individuele biometrische data). Desondanks worden beslissingen over grootschalige implementatie vaak genomen, voordat systemen volledig zijn getest. Bij het voorgestelde ID-systeem in het Verenigd Koninkrijk, bijvoorbeeld, wordt verwacht dat maar liefst één op de zes personen hun identiteitskaarten niet zal kunnen gebruiken vanwege de FTE problemen.[41] Soortgelijke problemen zijn ook te constateren bij opsporingstechnieken, zoals gezichtsherkenning en ANPR.

Technologische insluiting en trage wetgeving: Bewakingstechnologieën worden vaak zonder problemen aangeprezen als 'het antwoord' op allerlei bedreigingen, zoals de recente terrorisme dreiging. Hoe meer we echter afhankelijk worden van bewakingstechnologie, hoe meer er sprake lijkt te zijn van een 'insluiting' die het overwegen van andere mogelijkheden uitsluit, en van een kenniskloof die de afhankelijkheid van expertise buiten het democratische systeem vergroot. Wetgevers lopen voortdurend achter bij de technologische ontwikkelingen en geven ervan blijk geen inzicht te hebben in 'hoe het werkt'. Bij deze voortdurende wedloop is de vraag gerechtvaardigd of overheden wel over de nodige middelen beschikken om belangrijke wetgeving rond complexe bewakingssystemen tot stand te brengen. De vraag die in verband met de snelle technologische ontwikkeling vaak opkomt is of 'de geest niet weer terug in de fles kan worden gestopt'. Octrooihouders en leveranciers doen er meestal het zwijgen toe als het gaat over de omkeerbaarheid van apparaten en systemen.

Bewakingsprocessen

Het belang van preëmptieve risicoanalyse en het voorschrijven van bewaking als oplossing voor allerlei problemen heeft geleid tot het ontstaan van diverse nieuwe, aan bewaking gerelateerde processen en verschijnselen. Het indelen in groepen, onvoorziene gevolgen, het delen van informatie en het vervagen van de grenzen van het publieke en private domein zijn enkele voorbeelden.

Indelen in groepen, categoriseren en gerichtheid op doelgroepen. Het indelen van de bevolking in verschillende groepen naar risico, rechten of waarde is op veel gebieden waar te nemen:

- Consumenten zijn voortdurend bezig bedrijven te voorzien van hun transactiegegevens en vormen onderdeel van een feedback lus waarin koopgedrag is gekoppeld aan het verzamelen van gegevens en het genereren van profielen.[42] Callcenters delen klanten tegenwoordig in op basis van uitgavenpatroon en passen hun serviceniveaus daaraan aan. De telecomindustrie registreert telefoonverkeer om de snelste 'weg naar de markt' te vinden (bijvoorbeeld marketing via SMS).

---

[39] Hampapur, A. *et al*. (2005), 'Smart video surveillance', *IEEE Signal Processing Magazine*, March: 38-51.
40 Zie: Zureik, E. en Hindle, K. (2004) 'Governance, security and technology: the case of biometrics' Studies in Political Economy, 73: 113-137.
41 Zie: Grayling, A.C. (2005) In Freedom's Name: The Case Against Identity Cards, London: Liberty.
42 Uiteengezet in: Elmer, G. (2004). Profiling Machines: Mapping the Personal Information Economy. Cambridge, MA: The MIT Press.

- Callcenter-medewerkers worden geselecteerd op basis van hun sociale vaardigheden en levensstijl, zodat ze het best passen bij de doelgroep die ze gaan bedienen.
- Op veel aankomsthavens is het tegenwoordig mogelijk om de paspoortcontrole versneld te passeren, bijvoorbeeld het 'Privium' irisscan systeem op Schiphol.

Onbedoelde controle: Bewaking moet niet worden verward met directe sociale controle.[43] De bedoeling van bewaking is vaak alleen om de doorstroom van goederen, mensen en informatie snel en efficiënt te laten plaatsvinden.[44] Wat de een betitelt als 'efficiency', wordt door de ander echter vaak opgevat als 'sociale controle': dit geldt met name voor sterk gepersonaliseerde systemen, bijvoorbeeld voor het opvragen van identiteitsgegevens, die werken op basis van unieke identificatoren gekoppeld aan individuele burgers.[45]

Informatie delen: Om mensen in groepen te kunnen indelen is nauwkeurige, snel toegankelijke informatie nodig. In veel landen, waaronder het Verenigd Koninkrijk, is een trend zichtbaar naar meer geïntegreerde, 'gekoppelde' openbare diensten, vaak via samenwerking met diverse dienstverlenende bedrijven. Steeds vaker is op lokaal niveau sprake van samenwerkingsverbanden, waarbij verschillende dienstverleners en beroepen betrokken zijn, met als doel de dienstverlening te verbeteren door een meer geïntegreerde aanpak.[46] Een van de gevolgen van deze belangrijke ontwikkeling is dat er twijfel is ontstaan over de grenzen die tot nu toe de privacy toch tot op zekere hoogte beschermden en bewaking min of meer afbakenden, met als gevolg dat zowel bij overheidsdiensten als dienstverleners grote verwarring bestaat over de manier waarop persoonsgegevens (zouden moeten) worden beheerd.[47] Deze ontwikkeling doet zich voor bij overheidsdiensten, rechtshandhavers, grenscontrole en marketing. Nectar van Loyalty Management UK, bijvoorbeeld, voorziet meer dan 50% van de Britse bevolking van een klantenkaart. 216 postorderbedrijven in het Verenigd Koninkrijk zijn lid van het Abacus data-sharing consortium dat over gegevens van 26 miljoen individuele consumenten beschikt in combinatie met de Claritas Lifestyle Universe database. Dit levert van al deze consumenten informatie op over hun inkomen, levensstijl en levensfase.[48]

Het vervagen van de grenzen tussen de publieke en private sector: Hoewel zowel de publieke als de private sector informatie delen, vervagen de grenzen tussen de belangen van de overheidssector en de private sector, doordat steeds meer overheidstaken worden uitgevoerd door een soms ingewikkelde combinatie van overheidsdiensten, particuliere bedrijven, vrijwilligersorganisaties en marktmechanismen. Steeds vaker is op lokaal niveau sprake van samenwerkingsverbanden, waarbij verschillende dienstverleners en beroepen betrokken zijn, met als doel de dienstverlening te verbeteren door een meer geïntegreerde aanpak.[49]Waar overheidsgegevens beschikbaar zijn voor gebruik door particuliere bedrijven, wat bijvoorbeeld wordt beoogd met het National Identity Register (NIR), dient

---

[43] Lianos, M. (2001) Le Nouveau Contrôle Social: toile institutionnelle, normativité et lien social. Paris : L'Harmattan-Logiques Sociales.

[44] Graham, S. and Wood, D. (2003) 'Digitising surveillance: categorisation, space and inequality,' *Critical Social Policy*, 23: 227-248.

[45] Een kritisch verslag van een computerexpert: Clarke, R. (2006) 'National identity cards? Bust the myth of 'security über alles'!', http://www.anu.edu.au/people/Roger.Clarke/DV/NatID-BC-0602.html

[46] 6, P., Raab, C. and Bellamy, C. (2005) 'Joined-up government and privacy in the United Kingdom: Managing tensions between data protection and social policy, Part I'. *Public Administration* 83 (1): 111-133; Bellamy, C., 6, P., and Raab, C. (2005) 'Joined-up government and privacy in the United Kingdom: Managing tensions between data protection and social policy, Part II'. *Public Administration* 83 (2): 393-415.

[47] Een recent adviesrapport voor Binnenlandse Zaken vraagt om meer bevoegdheden in de strijd tegen de georganiseerde misdaad en financiële fraude en klaagt dat 'het delen van informatie met andere partijen in de publieke sector zeer fragmentarisch is, terwijl het delen van informatie tussen publieke en private sector zelfs nauwelijks wordt geprobeerd'. Het rapport dringt aan op verbetering van deze informatiestromen, waaronder – in verband met de Rapportering van Verdachte Activiteiten – het matchen van de informatie van het nieuwe Serious Organised Crime Agency (SOCA) met de databases van allerlei overheidsdiensten, zoals Her Majesty's Revenue and Customs, de Driver and Vehicle Licensing Agency, DWP, en de Dienst Paspoorten. Er worden nu nieuwe initiatieven genomen, zoals de nieuwe Ministerial Committee on Data-Sharing, MISC 31, met de opdracht 'de strategie van de overheid te bepalen met betrekking tot het delen van informatie in de publieke sector'.

[48] Evans, M. (2005) 'The data-informed marketing model and its social responsibility.' in Lace, S (2005) *op cit*., n.3.

[49] 6 *et al*. 2005 *op cit*. n.24; Bellamy *et al*., 2005 *op cit*. n.46.

men zich af te vragen in hoeverre dit de goedkeuring wegdraagt van burgers en consumenten en waar de grenzen liggen. De privatisering van telecombedrijven, grensbewaking (IBM's Project Semaphore, het e-borders programma in het VK) en buurtpreventie (Citizen Corps in de VS, bijvoorbeeld, die 'letten op ongebruikelijke activiteiten') zijn bijvoorbeeld gebieden die ruimte laten voor twijfel.

Sociale gevolgen van bewaking

We zullen nu dieper ingaan op de sociale gevolgen van de bewakingssystemen en –processen die we tot nu toe hebben besproken. De kritiek op bewaking heeft meestal betrekking op de privacy en dat is inderdaad een belangrijk punt, maar we spreken in dat verband liever over één aspect van de autonomie van het individu. We willen ook de veel minder vaak besproken gevolgen voor de vrije keuze van mensen en het geven van goedkeuring onder de aandacht brengen; en, wat nog belangrijker is, de gevolgen van indeling, categorisering en doelgerichte marketing voor de levenskansen van mensen, groepen of gemeenschappen, hun relatieve mobiliteit en hun mogelijkheden om kansen te benutten.

Autonomie: Anonimiteit en Privacy: Bewaking tast de autonomie aan door inbreuk te maken op de anonimiteit en privacy van personen. Anonimiteit biedt mensen op allerlei manieren de mogelijkheid hun eigen identiteit te ontwikkelen op basis van hun doen en laten en relaties. Preventieve bewaking en met name identificatiesystemen tasten allereerst de anonimiteit aan die mensen in staat stelde de intensieve sociale controle in kleine gemeenschappen te ontvluchten. De privacy van kwetsbare of gemarginaliseerde groepen is aan voortdurende uitholling onderhevig. In Britse gevangenissen zijn veroordeelden integraal onderworpen aan een vrijwel continue bewaking. Zelfs na hun vrijlating worden (ex-)veroordeelden in toenemende mate onderworpen aan elektronische bewaking, als voorwaarde voor vervroegde vrijlating onder het Home Detention Curfew Scheme[50] of als voorwaarde voor voorwaardelijke vrijlating.[51] De praktijken van werkgevers die graven in het privé-leven van hun werknemers dienen voortdurend in de gaten te worden gehouden. Het spitten in meerdere databases door nationale identificatiesystemen, met name systemen die de publieke en de private sector koppelen, is een ontwikkeling die ernstige zorgen baart. Eind 2002 rapporteerde de BBC bijvoorbeeld dat opsporingsdiensten bij exploitanten van mobiele netwerken al meer dan 400.000 aanvragen voor het leveren van informatie over telefoonverkeer hadden ingediend.[52]Zoals de ACLU in zijn onderzoek ten behoeve van een nieuw bewakingsnetwerk opmerkte: bedrijven en burgers worden 'ingelijfd bij de bouw van een bewakingsstaat'.[53]

Keuze en toestemming: Keuze heeft een belangrijke rol gespeeld in de discussies over bewaking en gegevensbescherming in Noord-Amerika. In het Verenigd Koninkrijk is dit onderwerp echter enigszins ondergesneeuwd vergeleken met andere vormen van bescherming. Kunnen mensen, die een normaal leven willen leiden, kiezen of ze al dan niet worden bewaakt? Hoe kan men beweren dat we onze toestemming hebben verleend voor bewaking? Dit wordt het best geïllustreerd, als we zien hoe ons rechtssysteem omgaat met keuze. Het is niet onze vrije keuze dat we in de openbare ruimte door CCTV-systemen worden bewaakt en niemand heeft ervoor gekozen dat het ANPR-centrum van de ACPO de bewegingen van zijn/haar voertuig registreert. Arrestanten kiezen er niet voor, maar worden gedwongen hun vingerafdrukken en DNA-monsters te geven, die permanent worden opgeslagen in nationale politiedatabanken, ook als ze zonder veroordeling op vrije voeten worden gesteld. Hoewel mensen niet kunnen worden gedwongen urine af te staan om drugsgebruik te controleren, betreft dit toch nauwelijks een vrije keuze, want weigering kan immers resulteren in een boete, gevangenisstraf of beide. Voor burgers is het vrijwel onmogelijk erachter te komen hoe informatie wordt gebruikt en hoe die informatie, op subtiele wijze, hun levens beïnvloedt; bijvoorbeeld door de kans te verhogen

[50] Het Home Detention Curfew Scheme maakt het mogelijk veroordeelden tot een gevangenisstraf van drie maanden tot vier jaar twee weken tot vier en een halve maand eerder vrij te laten onder een avondklokregime dat door elektronische bewaking wordt gehandhaafd. In 2004/5 werden 19.096 veroordeelden onder deze regeling eerder vrijgelaten. Zie: NPS (2006) *op cit.* n. 82.

[51] ibid.

[52] 'Telefoonbedrijven 'overstroomd' met misdaadcontroles'. *BBC News*, 20 december 2002, http://news.bbc.co.uk/1/low/uk/2592707.stm

[53] Stanley, J. (2004) *The Surveillance-Industrial Complex*, Washington DC: ACLU. http://www.aclu.org/FilesPDFs/surveillance_report.pdf

dat hun voertuig door de politie wordt aangehouden of door van ze te verlangen dat ze vooruit betalen voor goederen en diensten. Een oplossing zou kunnen zijn om waar mogelijk de overheidscontrole op burgers niet-verplicht te maken, zoals in het Verenigd Koninkrijk wordt voorgesteld in verband met identiteitscontrole. Dit is echter een grotendeels illusoire oplossing, want als die controle nodig is om toegang te krijgen tot allerlei diensten, wordt het *de facto* verplicht. Bestaande identificatoren hebben bovendien betrekking op de specifieke functies van afzonderlijke groepen, zoals autorijders, consumenten of toeristen, terwijl het identiteitskaartsysteem de overheid in staat stelt activiteiten te bewaken van mensen in al deze hoedanigheden, inclusief die van burger.

Discriminatie: snelheid, toegang en sociale uitsluiting: Discriminatie in de vorm van verschillende snelheden van behandeling, snellere toegang tot diensten en diverse vormen van sociale uitsluiting zijn belangrijke gevolgen van de sociale indelingsprocessen die bewaking in het leven roept. Het overheidsdenken is veranderd. Waar in de vorige eeuw nog een burgerschapsconcept werd gehanteerd dat ervan uitging dat alle zich daarvoor kwalificerende personen moesten worden *opgenomen* in de systemen die in de gezondheidszorg, door de sociale dienst en gerechtelijke instanties worden gebruikt, wordt er tegenwoordig van uitgegaan dat het *uitsluiten* van ongewenste elementen van opname in dit soort systemen, waaronder identificatiesystemen, belangrijker is.[54] Wie toegang heeft tot de juiste systemen is uiterst mobiel – zoals internationale zakenmensen en toeristen – en hun identificatiesystemen (van creditcards tot 'frequente vlieger'-kaarten) lijken hun bewegingsvrijheid juist te bevorderen. Maar voor anderen, bijvoorbeeld gastarbeiders (of, erger nog, werkloze illegalen), vluchtelingen of asielzoekers, om niet te spreken van mensen met duidelijke 'islamitische' of 'Arabische' namen, lijken deze systemen de vrijheid van beweging te beperken, zowel in als tussen landen.

De toegenomen bewaking in steden heeft ook geleid tot ongebreidelde vormen van sociale uitsluiting. Bepaalde groepen en gebieden die als onrendabel of risicovol worden aangemerkt, worden buitengesloten. De nieuwe bewakingstechnologie draagt er op die manier juist toe bij dat bepaalde groepen ernstig worden *beknot* in hun levenskansen, met als gevolg datdeze in plaats van minder problematisch juist meer problematisch worden. Als ze eenmaal zijn geïmplementeerd, kunnen toegang en uitsluiting in steeds sterkere mate automatisch worden gecontroleerd,[55] waardoor een technologische insluiting dreigt te ontstaan die de moderne samenleving nog drastischer opsplitst in groepen van mensen die zich snel kunnen verplaatsen en 'aangesloten' zijn en groepen die zich moeilijk kunnen verplaatsen en 'uitgesloten' zijn. Uitsluiting is ook terug te vinden in de prijsklassen van goederen. Amazon.com biedt dvd's aan verschillende groepen consumenten aan voor verschillende prijzen, zodat de vraag gerechtvaardigd is of overheidsingrijpen nodig is om prijsafspraken over massaconsumptiegoederen de kop in te drukken. Hoewel het moeilijk is om conclusies te trekken over werkplekbewaking en sociale uitsluiting, vooral vanwege de bestaande indeling in beroepsgroepen en sociale klassen op de arbeidsmarkt, lijkt er op één gebied duidelijk sprake te zijn van bevoordeling: e-recruitment. Wanneer grote aantallen cv's worden doorgespit op zoek naar geschikte kandidaten, komt de vraag of hier sprake is van discriminatie op twee manieren aan de orde. In de eerste plaats is e-recruitment gevoelig voor vooroordelen en 'nattevingerwerk', alleen al vanwege de keuze van de zoekopdracht, [56] [57] en in de tweede plaats hebben bepaalde maatschappelijke, economische en etnische groepen niet gemakkelijk toegang tot het internet.

Dit kan diep doorwerken in de infrastructuur van de samenleving. Als we constateren dat het menselijke beoordelingsvermogen wordt uitgesloten en door software wordt vervangen en dat culturele identiteit en volksaard worden omgeven met negatieve connotaties en verzwaard met een ballast van kansen, keuzen, herinneringen en verwachtingen, is het ironisch om te zien dat

[54] Bigo, D. (2004) 'Globalized in-security: the field of the professionals of unease management and the ban-opticon,' *Traces*, 4.
[55] Lianos, M. (2001) *op cit* . n.109; Lianos, M. (2003) 'Social control after Foucault,' *Surveillance & Society* 1(3): 412-430. http://www.surveillance-and-society.org/articles1(3)/AfterFoucault.pdf .
[56] Tversky, A. and Kahneman, D (1974) 'Judgement under uncertainty: heuristics and biases,' *Science* 185(4157): 1124-1131
[57] Mohamed, A.A., Orife, J. en Wibowo, K. (2002) 'The legality of key word search as a personnel selection tool,' *Employee Relations* 24(5).

tegelijkertijd wordt geprobeerd die identiteit te vangen in machineleesbare formules en algoritmes om bureaucratische verwerking, opsporing en bedrijfsadministratie te vereenvoudigen.

Democratie, verantwoordingsplicht en transparantie: Dit onderwerp roept veel vragen op: wat zijn de grenzen aan de controle door de overheid? Hoe moet de grens tussen commerciële databases en openbare veiligheid/staatsveiligheid worden gereguleerd? Hoe kunnen particuliere bedrijven aansprakelijk worden gesteld voor fouten en mismatches in hun databasesystemen? Tegenwoordig is het bijvoorbeeld zo dat burgers die op een 'smart border' controlelijst staan allerlei beperkingen opgelegd krijgen. Terwijl allerlei bedrijven en overheidsdiensten toegang hebben tot het systeem of gegevens in het systeem kunnen invoeren, zijn de mogelijkheden om gegevens te verwijderen of te corrigeren beperkt. Ten slotte kunnen er ook grote vraagtekens worden gezet bij de verantwoording die gekozen regeringen aan hun burgers moeten afleggen en bij de 'offshore' aard van allerlei particuliere leveranciers van de huidige bewakingssystemen. Commerciële databanken van multinationals met creditcard transactiegegevens of informatie over mobiel telefoonverkeer kunnen in feite 'offshore' zijn, buiten het bereik van de rechtsstaat. Recente voorbeelden van multinationals die informatie uitleveren stellen bepaalde eisen aan overheidscontrole en regulering, vooral wanneer een bedrijf *zowel* de commerciële gegevens in eigendom heeft *als* een contract heeft voor de levering van bewakingssystemen.

Volgens de wetgeving in veel landen hebben burgers het recht te weten welke gegevens over hen worden bijgehouden en hoe deze worden gebruikt, hoewel daarop uitzonderingen zijn. Dit recht vereist dat een 'data controller' elke burger informeert over de over hem/haar opgeslagen gegevens en over de verwerking daarvan. Hierdoor zou de scheefgroei tussen het almachtige oog van de overheid en de rechten van de burger enigszins worden gecorrigeerd, vooral waar toestemming voor het gebruik van onze persoonsgegevens wordt geïmpliceerd, maar niet uitdrukkelijk is verleend. Veel mensen kennen hun rechten echter niet, oefenen deze niet uit en krijgen weinig hulp van anderen om ze daarbij te helpen.

Intensieve dataveillance is een normaal verschijnsel aan het worden in de moderne samenleving en is op zichzelf te rechtvaardigen – en wordt door voorstanders dan ook op die manier gerechtvaardigd - in naam van het algemeen belang. Voor deze activiteiten hebben parlementen vaak uitdrukkelijk toestemming verleend. Wat ze problematisch maakt, is dat ze grote hoeveelheden persoonsgegevens verwerken op wijzen die de grenzen overschrijden die zijn bepaald door de beginselen van gegevensbescherming, door de wetgeving op het gebied van de bescherming van persoonsgegevens (ook via het parlement) en door andere beperkingen en richtlijnen die gelden voor het verzamelen, verwerken en doorgeven van informatie. We kunnen eraan gewend raken dat we worden bewaakt, dat ons doen en laten in de gaten wordt gehouden en zelfs geanticipeerd, zonder dat we het merken en – vooral waar het openbare diensten betreft – zonder de mogelijkheid te hebben onze toestemming al dan niet te verlenen of zonder volledig inzicht te hebben in wat er met onze gegevens gebeurt. Mogelijk aanvaarden we beperkingen van onze privacy als 'redelijk', waar we deze zouden afkeuren, wanneer we ons rekenschap zouden geven van wat burgerschap inhoudt. Het is verre van zeker dat het politieke bestel uiteindelijk zorgt dat ons recht op privacy krachtig wordt gehandhaafd en beschermd tegen het beroep van overheidsdiensten op het 'algemeen belang', ook waar dit algemene belang duidelijk lijkt en prioriteit kan hebben. Als bewaking binnen 'proporties' moet blijven, hangt het er maar van af hoe die term wordt geïnterpreteerd en wie dat doet. Veel hangt ook af van de beschermende maatregelen rond de nieuwe, binnendringende ontwikkelingen.

4. Regulering van de bewakingsstaat

Bewaking vergt regulering. Onder ‘regulering’ verstaan we niet alleen wetgevende maatregelen om systemen en praktijken te reguleren, maar alle maatregelen die een regulerend effect hebben[58]: dat wil

[58] Baldwin, R. and Cave, M. (1999) *Understanding Regulation: Theory, Strategy and Practice*. Oxford: Oxford University Press.

zeggen, ze leggen regels op aan bewaking en gegevensverwerking door grenzen te bepalen en controles in te bouwen. De meeste systemen voor het beheer van de verwerking van persoonsgegevens zijn ontwikkeld in de context van gegevensbescherming met de bedoeling de *privacy* te beschermen. Onze opmerkingen in dit hoofdstuk hebben vooral betrekking op deze strategieën. Het reguleren van *bewaking* zou wel eens moeilijker kunnen zijn dan het lijkt. Er valt iets voor te zeggen om de wettelijke bescherming tegen bewaking apart te ontwikkelen, omdat de ongewenste effecten ervan niet alleen te maken hebben met inbreuk op privacy en omdat de eerste afweerlinie misschien niet verwaarloosbaar is, maar wel kwetsbaar. In dit deel van het rapport gaan we nader in op de bestaande wetgeving en beoordelen we de effectiviteit daarvan. Ook doen we suggesties voor verbetering.

Wat is er mis met regulering?

De regulering van privacy en bewaking heeft te lijden gehad van bepaalde algemene nadelen. We kunnen hier ten minste zes probleempunten onderscheiden:

- De regulering is vaak reactief: er is 'achteraf' gereageerd op technologische ontwikkeling, implementatie en uitoefening.
- Regulering heeft zich grotendeels gericht op techniek en beheer, op basis van aanvaarde normen, de nakoming van wettelijke standaardvoorschriften en de toepassing van privacy beschermende technologie, wat weinig ruimte laat voor anticipatie.
- Veel regulering is gebaseerd op een beperkte notie van persoonlijke privacy en van de waarde daarvan voor de individuele burger, (noodzakelijkerwijs) voortkomend uit het huidige gedachtegoed van beleidsmakers die vaak een beperkte visie hebben op wat in het 'algemeen belang' is.
- Regulering is een onderwerp waarover de discussie zich grotendeels buiten het domein van het openbare debat afspeelt. De discussie wordt gevoerd door experts: bijvoorbeeld op het gebied van gegevensbescherming of rechtshandhaving. Dit heeft tot gevolg gehad dat de 'gewone man' nauwelijks betrokken is geweest bij enkele van de belangrijkste vraagstukken van onze tijd .
- Regulering wordt vaak – in politieke termen – beschouwd als een juk dat ten onrechte is geplaatst op de schouders van het bedrijfsleven en de overheid en dat initiatief, ondernemen en productiviteit belemmert. In het VK is geprobeerd die last te verlichten door duidelijke pogingen tot deregulering of 'betere regulering'. Het inzicht dat zowel het bedrijfsleven als de overheid kan profiteren van het grotere vertrouwen bij de burger en de verbeterde efficiency als gevolg van een goede regulering, wordt ,hoewel vaak met de mond beleden, in de praktijk door weinigen gedeeld.
- De discussie in de media is vooral gericht op 'griezelverhalen' over gevallen van inbreuk op de privacy en het schetsen van zowel de utopische als de Orwelliaanse kanten van de bewakingstechnologie. Actuele nieuwsberichten zijn belangrijk, maar de complexe ethische en sociale problematiek rond bewaking wordt maar al te vaak genegeerd. De discussie over bewaking beperkt zich vaak tot het bespreken van oorzaak en gevolg ('CCTV voorkomt misdaad') of tot angstvisioenen ('we worden allemaal in de gaten gehouden'). Zo worden andere zienswijzen ook vaak getorpedeerd door het gevaarlijke schijnargument 'wie niets te verbergen heeft, heeft ook niets te vrezen'.

De huidige staat van regulering

De afgelopen 35 jaar is de bescherming van de privacy een wereldwijde issue geworden. De kern van dit verschijnsel wordt gevormd door een paar totemistische principes. Deze schrijven voor dat een organisatie:

- *verantwoordingsplicht* heeft voor alle persoonsgegevens die het in bezit heeft.
- *het doel* waarvoor de informatie wordt verwerkt duidelijk moet maken op of voor het tijdstip van verzamelen;

- alleen persoonsgegevens mag verzamelen van personen die daarvan *op de hoogte zijn en daartoe toestemming hebben verleend* (bijzondere omstandigheden uitgezonderd).
- het *verzamelen van persoonsgegevens strikt dient te beperken* tot het beoogde doel.
- persoonsgegevens niet mag gebruiken of openbaar mag maken voor andere doelen dan de bekend gemaakte doelen, tenzij de betreffende persoon daar toestemming voor heeft verleend (het *finaliteits*principe);
- informatie alleen dient te *bewaren* zo lang als dit nodig is;
- dient te zorgen dat persoonsgegevens *nauwkeurig* worden bijgehouden, *volledig* en *up-to-date* zijn;
- persoonsgegevens dient te beschermen met gepaste *veiligheidsmaatregelen*;
- *transparantie* dient te geven over het privacy-beleid en zich dient te onthouden van het aanhouden van een systeem met geheime informatie
- de betrokkenen *toegang* dient te verschaffen tot hun persoonsgegevens en hen in staat moet stellen deze te wijzigen, wanneer de gegevens onjuist, onvolledig of verouderd zijn.[59]

Onder de druk van deze of soortgelijke 'fair information principles' (FIPs), is de wereld van wet- en regelgeving aangaande aantasting van privacy en bewaking bevolkt door algemene wetten, wetten voor bepaalde sectoren (zoals telecommunicatie) of praktijken (zoals data matching) en internationale documenten en verklaringen op wereldwijde of regionale schaal, waarvan wellicht als meest opvallende de Europese Privacy Richtlijn 95/46/EC, ook genoemd in de Richtlijn betreffende Privacy en Elektronische Communicatie (2002/58/EC), kan worden genoemd. Regelgevende instanties, zoals privacytoezichthouders, zijn ingesteld op nationaal, subnationaal en zelfs regionaal niveau. Daarnaast hebben particuliere bedrijven, brancheorganisaties en overheidsdiensten hun eigen gedragscodes en protocollen opgesteld en hebben online bedrijven privacyverklaringen opgesteld of privacybeleid ontwikkeld. Boetes en sancties zijn opgelegd aan overtreders op grond van de diverse vormen van wet- en regelgeving. De afgelopen jaren zijn technologische oplossingen – privacy bevorderende technologie (PET) – aangedragen om te pogen het verzamelen van informatie te beperken en anonimiteit te beschermen en om de bewakingscapaciteit van de technologie zelf af te zwakken. Voorvechters van privacy hebben luid en duidelijk gewaarschuwd voor de gevaren, praktijken aan de kaak gesteld en het publiek geïnformeerd over de gevolgen van bewaking en inbreuk op privacy voor hun bestaan. De media hebben vaak gereageerd op de bedreigingen van bewaking, ook al vinden media het zelf vaak lonend om de privacy van zowel beroemdheden als 'gewone' burgers te schenden.

Een praktisch stelsel te bouwen op het smalle fundament van privacy- en gegevensbescherming lijkt velen een doodlopende weg. Anderen[60] zijn echter van mening dat privacy en de bescherming daarvan zich kunnen uitstrekken tot andere, fysiek indringende situaties waarin sprake is van een scheve verhouding tussen het individu en de bewakers, zoals bij videobewaking. Nieuwe bewakingspraktijken leiden echter in toenemende mate tot discriminatie en andere sociale 'kwaden' met ernstige en kwalijke gevolgen voor de maatschappelijke kansen van mensen, die buiten het domein liggen van inbreuken op de privacy die vaak tot individuen beperkt zijn. Er valt daarom iets voor te zeggen de wet- en regelgeving op het gebied van bewaking en privacy te herzien en aan te passen (ten minste) om het ontwerpen en implementeren van nieuwe, intensievere en uitgebreidere bewakingstechnieken aan banden te leggen en de gevolgen daarvan te beperken. De nieuwe bewaking betreft echter niet alleen technologie. Het 'probleem' van wet- en regelgeving heeft wellicht niet alleen te maken met de manier waarop de technologie kan worden aangepakt, maar ook met de manier waarop het beleid en de doelstellingen kunnen worden beïnvloed van de bedrijven die ze ontwikkelen en toepassen en de manier waarop samenlevingen en bevolkingen die eraan worden onderworpen kunnen worden beïnvloed.

[59] Bennett, C. and Raab, C. (2006) The Governance of Privacy: Policy Instruments in Global Perspective, Cambridge MA: MIT Press, 12.
[60] bijvoorbeeld: Dubbeld, L. (2004) The Regulation of the Observing Gaze: Privacy Implications of Camera Surveillance. Enschede: Ipskamp Printpartners.

Regelgevende instrumenten: de voors en tegens

Het bestaande repertoire van beleidsinstrumenten dat wordt toegepast op de bescherming van privacy en persoonsgegevens en dus ook in hoge mate op bewaking van toepassing is, is als volgt:[61]

Internationale instrumenten: Het Europese Verdrag tot bescherming van de Rechten van de Mens en andere internationale verklaringen verlenen de bescherming van privacy een wettelijk en moreel kader dat een belangrijke rol kan spelen bij het beteugelen van de uitwassen van bewaking. Deze en aanverwante documenten hebben vorm gegeven aan bepaalde wetgeving en de invoering daarvan in een zeer groot aantal landen en in een beperkt aantal rechtsgebieden. Maatregelen op internationaal niveau zijn grotendeels verantwoordelijk voor de uitstekende kwaliteit van de beginselen die al zo lang ten grondslag liggen aan gegevensbescherming en - in het verlengde daarvan – van bewaking.

Wetten: Sinds de jaren zeventig heeft de wetgeving om de verwerking van persoonsgegevens aan banden te leggen een grote vlucht genomen. Veel landen hebben sectorale en algemene wetten op het gebied van gegevensbescherming aangenomen en de meeste van die wetten hebben geleid tot een bepaalde vorm van handhaving en supervisie. Wat het laatste betreft, spelen bijvoorbeeld de privacytoezichthouders een essentiële rol om de privacy te beschermen. De VS houdt zich afzijdig van de 'club' van landen met uitgebreide wetten op dit gebied, wat de inspanningen om te komen tot een wereldwijde regelgeving op het gebied van bewaking verzwakt en leidt tot fragmentarische resultaten. De zwakte van veel wetten op het gebied van de verwerking van persoonsgegevens, en van de machinerie om die wetten in te voeren, is vaak aanleiding geweest tot klachten. Critici klagen terecht over wetgevende maatregelen die bewaking eerder legitimeren dan reguleren.[62] Bovendien is het niet gemakkelijk om met wetgeving op het gebied van privacy en gegevensbescherming allerlei bewakingstoepassingen te reguleren, zoals toepassingen die onderdeel vormen van moderne telecommunicatiesystemen, en is die wetgeving niet gemakkelijk universeel voor dat doel te interpreteren. Ook is het zo dat de schade die bewaking kan veroorzaken voor personen, groepen en hele samenlevingen, niet valt binnen het werkingsgebied waarvoor deze op individuele rechten gebaseerde, preventieve of corrigerende wetten zijn ontworpen.

Zelfregulering: Industrieën of bedrijven, overheidsdiensten en staten hebben allerlei gedragscodes of regels ontwikkeld om bewaking op allerlei gebieden te reguleren. Er bestaat ook online zelfregulering van op het internet actieve bedrijven in de vorm van online privacyverklaringen, gesteund door organisaties die deze bedrijven certificeren. Zelfregulering wordt soms opgenomen in wetgeving, evenals gedragscodes, zoals in de Data Protection Act 1998 (VK) en de Europese Privacy Richtlijn 95/46/EG. Zelfregulering wordt in toenemende mate beschouwd als een betere manier van regulering, gezien de 'onmacht' van wetten en de gewenste vermindering van de regulering voor het bedrijfsleven.[63] Toch kunnen gedragscodes en dergelijke moeilijk bestaan zonder een bestaand of gelijktijdig ontwikkeld kader van wetten of internationale regels waaruit de normen en richtlijnen voor gedragsregels worden afgeleid.

Privacy-bevorderende technologie: Een belangrijke ontwikkeling sinds het begin van de jaren negentig is het besef dat juist technologie krachtige middelen kan opleveren om de bewakingspraktijk te controleren en de inbreuk op privacy te bestrijden. Of een bepaalde technologie geschikt is voor bewaking, hangt af van de manier waarop de technologie is ontworpen en wordt toegepast. De versleuteling van persoonsgegevens voor gegevenstransmissie tussen domeinen en over andere

[61] Zie voor een meer gedetailleerde typologie en bespreking *op cit.* n. 59: chs. 4-7.
[62] Flaherty, D. (1989) Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada, and the United States. Chapel Hill NC: University of North Carolina Press.
[63] US Department of Commerce, National Telecommunications and Information Administration (NTIA) (1997) *Privacy and Self Regulation in the Information Age*. Washington DC: Department of Commerce, NTIA.

grenzen, die kan variëren van niet-bestaand tot sterk ontwikkeld, kan in combinatie met netwerkdesign en softwarecode een sterk regulerend effect hebben.[64] Encryptie, anonieme web-browsing, filters, smart agents, privacy-preference tools, etc., kunnen krachtige middelen zijn om de privacy van personen te beschermen. Het is echter onduidelijk of deze instrumenten op zichzelf een krachtige oplossing bieden tegen online bewakingspraktijken.

Individuele zelfhulp: Dit is nog een breed terrein voor regulering. Gebruikers beheren de openbaarmaking van hun eigen gegevens, hetzij door het gebruik van PET's, hetzij door zich af of aan te melden voor bepaalde gegevensverwerkende procedures, maar ook door kennis van een waakzaamheid betreffende bewakingspraktijken en de bedreiging van inbreuken op de privacy. Al deze middelen zijn afhankelijk van de mate van belangstelling die een persoon heeft voor bescherming en de bewaking van 'cultureel kapitaal' – het vermogen en de middelen om te begrijpen wat er gebeurt en zich in te spannen om zich te verweren tegen inbreuken of verhaal te halen wanneer deze bedreigingen reële vormen hebben aangenomen. Bij ontstentenis van regelgevende of toezichthoudende lichamen, is in de VS zelfhulp, het nemen van rechtsmaatregelen inbegrepen, het meest gebruikte middel van privacyregulering en de kritiek op deze situatie is dan ook niet van de lucht. Andere systemen van gegevensbescherming zijn tot op zekere hoogte afhankelijk van personen die bij de wetgevers klagen en fungeren als klokkenluiders die dubieuze praktijken aan de kaak stellen.

De volgende activiteiten zijn in dit verband ook relevant:

- privacy en anti-bewaking pressiegroepen die, evenals delen van de media, het grote publiek wijzen op problemen en risico's, situaties in de gaten houden en druk uitoefenen op overheden en bedrijven die bewaking toepassen.
- technologen die bewakings- en informatiesystemen ontwerpen en wier opleiding, training en naleving van gedragscodes van invloed kunnen zijn op de bewustwording van hun werknemers en bepalend zijn voor de producten die ze ontwikkelen;
- wetenschappers die kunnen toelichten wat er gebeurt, duidelijk kunnen maken waarom het gebeurt en theorieën kunnen ontwikkelen en testen over de plaats en de legitimiteit van bewaking in de samenleving, in het verleden, het heden en de toekomst en op die manier hun kennis beschikbaar stellen aan het openbare debat.

Algemene problemen aangaande instrumenten

Drie van de belangrijkste problemen met de bestaande regelgevende praktijk hebben te maken met *fragmentatie* en *zwakke coördinatie*. Het ene probleem betreft de belangrijkste *instrumenten*, het andere de wirwar van wetgevende *niveaus* waarop regelgeving dient plaats te vinden. In beide gevallen heeft het probleem te maken met mogelijk hechtere, wereldwijde oppositie tegen regelgeving op het gebied van bewaking, wanneer de huidige trends zich voortzetten. In beide gevallen is het de vraag hoe een en ander kan worden verbeterd. Met andere woorden: kunnen we vuur met vuur bestrijden? Als de krachten die bewaking willen uitbreiden steeds verder worden geïntegreerd en 'gekoppeld', nationaal of internationaal, hoe goed geïntegreerd zijn dan de instrumenten en de niveaus die tegenwicht bieden aan beschermende acties of maatregelen? Het derde probleem heeft te maken met de toepassing van deze instrumenten op de sociale effecten van bewaking – en wellicht vooral van 'nieuwe bewaking' – buiten het terrein van privacy-inbreuk of van het ontwikkelen van nieuwe middelen. In alle drie de gevallen is er ruimte om het arsenaal van de regulering te heroverwegen en te bedenken hoe het coherenter en effectiever kan worden gemaakt. Er is ook ruimte om de mogelijkheden te overwegen van impactanalyse op het gebied van privacy en bewaking, toe te passen op welke niveau dan ook en op welk (toepassings)gebied of domein dan ook. Ook dit kunnen we hier alleen maar aankaarten.

Mogelijkheden voor toekomstige regulering

[64] Lessig, L. (1999) *Code and Other Laws of Cyberspace*. New York NY: Basic Books.

Privacy Impact Assessment: Wij zijn van mening dat de toepassing van Privacy Impact Analysis (PIA) in de regelgeving van rechtsgebieden op welk relevant niveau dan ook van grote waarde kan blijken te zijn.[65] PIA kan het best worden opgevat als een instrument dat partijen die nieuwe of herziene systemen voor de verwerking van persoonsgegevens voorstellen, kunnen gebruiken om de mogelijk schadelijke gevolgen voor personen te verlichten. PIA kan ertoe bijdragen duidelijkheid te verschaffen over de manier waarop privacybescherming binnen een omgeving waarin informatie wordt gedeeld, kan dienen als een belangrijk ethisch en juridisch middel om belangrijke sociale en politieke doelen juist te realiseren, zoals een betere, meer op de burger gerichte openbare dienstverlening of betere beveiliging, en daarvoor geen belemmering vormt.

Van Privacy Impact Assessment naar Surveillance Impact Assessment: Om de mogelijk schadelijke gevolgen van bewaking in een breder kader te plaatsen dan dat van de privacybescherming, lijkt het ons noodzakelijk om PIA-tools te ontwikkelen die uitstijgen boven hun huidige configuratie en zogenaamde *surveillance impact assessment* of SIA-tools te ontwikkelen. Dit vergt natuurlijk een wijziging van definitie, want waar PIA de gevolgen analyseert van *informatieverwerking voor de privacy*, analyseert SIA de gevolgen van *controle voor een reeks waarden*, waaronder privacy zelf.

Omdat PIA is ontwikkeld als middel om *privacy* te bewaken, in termen van individuele burgerrechten, is het op dit moment niet het meest geschikte middel om de verdere varianten van bewaking in een kader te plaatsen in termen van de diverse andere sociale en persoonlijke gevolgen. Dit zou een verandering van denken vereisen, waarbij niet alleen het effect op personen in aanmerking zou worden genomen, zoals bij privacybeleid vaak het geval is, maar ook de waarde van privacybescherming en de beperking van bewaking in termen van de samenleving.[66] Privacy is niet alleen een individueel goed, maar ook belangrijk voor de samenleving als basis voor het algemeen goed en gemeenschappelijke waarden, zoals democratie, vertrouwen, sociabiliteit en een maatschappij gebaseerd op vrijheid en gelijkheid. Omdat de waarde van privacy zich uitstrekt tot voorbij het individu, hebben we allemaal een aandeel in de rechten en de mogelijkheden van het individu om zijn privacy te beschermen. Het is een collectieve waarde, voorzover het een collectief goed betreft dat ondeelbaar is, dat een bescherming biedt waarvan niemand kan worden uitgezonderd en die de markt niet effectief kan bieden.[67] Om die reden zou SIA een waardevolle rol kunnen spelen door PIA te integreren, maar tegelijk te overstijgen met allerlei vormen van onderzoek gericht op het analyseren van de gevolgen van bewaking of de inbreuk op de privacy, op de samenleving zelf en op de andere, niet aan privacy gerelateerde belangen van afzonderlijke individuen, categorieën en groepen.

De vragen die bij een SIA aan de orde kunnen komen, zijn bijvoorbeeld:[68]

- Veroorzaakt de techniek ongerechtvaardigde fysieke of psychologische schade?
- Overschrijdt de techniek een persoonlijke grens zonder toestemming (al dan niet onder dwang of met bedrog, of al dan niet van fysieke of ruimtelijke aard)?
- Schendt de techniek aannamen over hoe persoonsgegevens behoren te worden behandeld (geen geheime opnamen)?

Andere opties: Als SIA is gebaseerd op PIA, komen ook andere opties in zicht.

- Een poel van technologische kennis opzetten om regelgevers te helpen de ontwikkelingen bij te houden.

[65] Stewart, B. (1999) 'Privacy impact assessment: towards a better informed process for evaluating privacy issues arising from new technologies,' *Privacy Law & Policy Reporter* 5 (8): 147-149; a descriptive discussion of PIA is given in Raab, C., 6, P., Birch, A. and Copping, M. (2004) *Information Sharing for Children at Risk: Impacts on Privacy*. Edinburgh: Scottish Executive.

[66] Regan (1995) *op cit.* n.9, ch. 8.

[67] ibid.

[68] Gary T. Marx, 'Ethics for a the New Surveillance', *The Information Society*, 14, 3, 1998: 174

- Managers en technologen adviseren hoe ze bewakingstechnieken op een verantwoorde manier kunnen ontwikkelen en implementeren, rekening houdend met strategie, organisatiestructuurveranderingen, training van werknemers en maatschappelijke verantwoordelijkheid
- Privacy herdefiniëren als een collectieve, maatschappelijke waarde in plaats van een individuele waarde.
- Het openbare debat over bewaking bevorderen op een participerende, niet paternalistische manier.
- Onafhankelijke analyses laten verrichten van de kosten van de naleving van privacyregels en bewakingswetgeving. Bekijken of de regels excessief zijn en of ze innovatie tegenhouden. Bekijken of hierdoor een beter evenwicht ontstaat tussen de voordelen van openbaar vertrouwen en efficiency, daarbij in aanmerking nemend dat de 'evenwicht'-test verre van adequaat is en op zichzelf in aanmerking komt voor nadere beschouwing.
- De toon van de media uittillen boven het niveau van clichés, sensatie en paniekzaaierij.

Ten slotte nog een opmerking over de manier waarop regulering zou kunnen worden verbeterd door de samenwerking en onderlinge samenhang van taken nader te beschouwen: tussen wetgevende instanties op verschillende niveaus tot en met internationaal niveau en tussen de verschillende deelnemers, zoals regelgevende instanties en maatschappelijke groepen. Het blijft een onderwerp van verdere discussie in hoeverre, bijvoorbeeld, de samenwerkingsverbanden genoemd in de EU Richtlijn 95/46/EG niet alleen de rechtshandhaving en de naleving hebben gediend, maar ook het verzamelen van informatie en de bewustwording op het bredere front van bewakingspraktijken en technologieën. In hoeverre is er, om nog een voorbeeld te noemen, een wederzijds vruchtbare relatie tussen wetgevende instanties en maatschappelijke groepen waar die instanties bij gebaat zijn, als die groepen problemen aankaarten of nuttige informatie of kennis aanbrengen en fungeren als klokkenluiders, wanneer regulering lijkt te falen of wanneer de overheid en het bedrijfsleven de bewaking lijken op te voeren. Of er ruimte is voor verdere innovatie wat betreft onafhankelijke bijdragen aan het regelgevende systeem, afgezien van toegewijde regelgevers en anti-surveillance voorvechters, is een vraag die buiten het bestek valt van dit rapport, dat als een soort illustratie daarvan kan worden beschouwd.