Inzicht en toezicht: controle in de kennissamenleving

Wolter Pieters, Kees Boersma, Gerard Alberts, Jaap Timmer, Anne Dijkstra en Marcus Popkema

Transparantie en controle lijken de adagia van deze tijd. Overlegorganen zijn in diskrediet geraakt, gegevens van kinderen moeten worden geregistreerd, onze bio-prints staan in onze identiteitskaarten en in internetdatabanken. Iedereen vraagt iedereen altijd en overal naar het legitimatiebewijs. Transparantie en controle leveren kennis op en vooral heel veel informatie. Wie doet wat, waarom met deze informatie en hoe? Met de toename van kennis hebben we steeds meer inzicht gekregen in de wereld om ons heen, en daarmee ook mogelijkheden om deze naar onze hand te zetten. Kennis en beheersing zijn altijd verweven geweest: techniek en wetenschap zijn steeds in elkaars buurt. Het lijkt daarbij in de eerste plaats te gaan om kennis als voorwaarde voor beheersing. De verhouding tussen kennis en beheersing is echter sinds het eind van de twintigste eeuw in een nieuw daglicht komen te staan. In de eerste plaats blijkt beheersing duidelijke grenzen te kennen, bijvoorbeeld wanneer het gaat om duurzaamheid. In de tweede plaats blijkt controle ook weer nieuwe kennis op te leveren, vooral in de vorm van toezicht. Dit vraagt om het opnieuw doordenken van de verhouding tussen kennis en beheersing. De vraag wat kennis is, wat inzicht is en wat informatie is, komt in iedere aflevering van het Jaarboek Kennissamenleving aan de orde. Dit jaar stellen we in het bijzonder de verhouding tussen inzicht en toezicht ter discussie.

Informatietechnologie maakt het mogelijk steeds meer gegevens op te slaan en te verwerken. Voor zover het data betreft over klimaat of botsingen in deeltjesversnellers is dit weinig omstreden. Het kan zelfs helpen duurzaamheidvraagstukken op te lossen. Maar er komen ook steeds meer gegevens beschikbaar over mensen, organisaties en overheden. De nieuwe generatie Internet – ook wel Web 2.0 genoemd – bestaat uit vormen van interactieve kennisuitwisseling. Het systeem van uitwisseling dat Internet heet, wordt maar zeer ten dele begrepen wanneer we het slechts voorstellen als kennisverwerving of inzicht. Het is ook toezicht. De overheid kijkt naar organisaties en burgers en burgers houden de overheid in de gaten. Het wederzijds toezicht roept een nieuwe vraag op, die naar sociale duurzaamheid. Transparantie, de toegenomen hoeveelheid zichtbaar gemaakte kennis en informatie, heeft ook haar schaduwzijden. Hoogleraar informatiebeveiliging Bart Jacobs, bekend van de stemcomputer en de OV-chipkaart, diagnosticeert dit proces als een omkering van selectie en collectie.[1] Werden oorspronkelijk gegevens verzameld als men wist welke data men nodig had, tegenwoordig worden op voorhand zo veel mogelijk data verzameld om pas daarna te kijken wat daarvan bruikbaar is en waarvoor. Zo wordt kennis niet langer verzameld om inzicht te krijgen in een bepaalde vraag, maar om toezicht uit te oefenen op een bepaald gebied. De maatschappij lijkt daarmee een soort ‘control freak’ te worden. Het zesde Jaarboek Kennissamenleving stelt de vraag waarom kennis voor inzicht meer en meer vervangen lijkt te worden door kennis voor toezicht, en wat dit betekent voor de kennissamenleving.

In het toezien voltrekken zich paradoxale tendensen. In de economie wordt marktwerking gepropageerd, maar tegelijkertijd betekent dit dat er toezicht nodig is op het functioneren van diezelfde markten, bijvoorbeeld in de telecom- en energiesectoren. In de wereld van de wetenschap leiden concurrentie tussen instellingen en de nadruk op contractonderzoek tot meer toezicht op de inhoud van het onderzoek. Uit de studie *Betrekkelijke betrokkenheid. Studies in sociale cohesie* (2008) van het Sociaal en Cultureel Planbureau klinkt de roep om meer cohesie in buurten en wijken. Niet alleen fysieke contacten, maar ook deelname aan

virtuele, sociale netwerken komen daarbij aan de orde. Tegelijkertijd brengt meer cohesie ook meer sociale controle met zich mee.

Toezicht werkt bovenal disciplinerend. Het besef van de *mogelijkheid* gezien te worden – de camera hoeft niet aan te staan – volstaat om af te dwingen dat men niet wil opvallen. De massale opslag en analyse van gegevens, althans de mogelijkheid daartoe, heeft een verder strekkend effect. Het gemiddelde gedrag gaat gelden als de norm, afwijkend gedrag als verdacht. Dit effect wordt actief nagestreefd in het zogenaamde 'profiling': het afleiden van de kenmerken van een persoon uit de over hem of haar beschikbare gegevens. Vaak komen deze gegevens beschikbaar in ruil voor een bepaalde dienstverlening, zoals bij de Albert Heijn bonuskaart. Privacy wordt daarmee iets dat uitgeruild kan worden. Wat gebeurt er met de kennis en informatie die dergelijk toezicht oplevert? Mag de kennis over het individu worden 'verplaatst' (bijvoorbeeld van databestand naar databestand) zonder toestemming van het individu?

Toezicht verandert daarnaast ook de ruimte. De toename van toezicht op de openbare ruimte is zichtbaar door de groeiende aanwezigheid van camera's. Maar toezicht in de kennissamenleving gaat verder. Het strekt zich uit tot de virtuele wereld van het Internet. En ten slotte is toezicht doorgedrongen tot de 'mind and body' van het individu. Toezicht komt steeds nader. 'Big brother' volstaat niet langer als metafoor, omdat deze gegevens in toenemende mate door individuen zelf beschikbaar worden gesteld. Het sociale netwerk bestaat precies daarin dat burgers zelf gegevens creëren en zo uitnodigen tot toezicht. Voor dergelijk 'informationeel exhibitionisme' wordt inmiddels door de overheid in een campagne gewaarschuwd. De waarschuwende rol van de overheid staat op gespannen voet met de registrerende rol, het vastleggen van steeds meer gegevens door diezelfde overheid.

Bepaalde vormen van toezicht kunnen leiden tot meer betrokkenheid. Voorbeelden hiervan zijn buurtpreventie, of het richten van webcams op interessante locaties in de natuur. Aan de andere kant kan juist dit toezicht leiden tot minder betrokkenheid, omdat immers toch alles al geregistreerd wordt, en daardoor individuele verantwoordelijkheid minder nodig lijkt te zijn. Het lijkt hier uit te maken *wie* er precies toezicht houdt, en of dat burgers, bedrijven of overheden zijn. Democratie vraagt dat het toezicht niet slechts één kant op zou kunnen en mogen werken. Het gebruik van middelen als de Wet Openbaarheid van Bestuur (WOB) door actiegroepen is een voorbeeld van toezicht op de overheid door burgers. De bezwaren tegen het elektronisch patiëntendossier laten zien dat de burger ook niet meer zomaar alles accepteert. Individuen en organisaties verzinnen ook zelf nieuwe manieren om toezicht te omzeilen. Ethische en juridische aanvaardbaarheid van toezicht zijn telkens een punt van discussie.

Het is duidelijk dat toezicht in de kennissamenleving nieuwe vormen aanneemt. Het gaat hierbij zowel om toezicht op individuen en organisaties op basis van 'algemene' wetenschappelijke kennis (u mag het strand niet op want er komt storm, u moet een prik halen) als om toezicht op basis van gedetailleerde gegevens over (rechts)personen (u koopt te vette producten). Dit Jaarboek spoort de nieuwe verschijningsvormen van toezicht in de kennissamenleving op. Welke rollen spelen burgers, overheid en bedrijfsleven? De technische middelen veranderen, sterker nog, ze veranderen de verhoudingen tussen burger en overheid. Inzicht of kennis is van karakter veranderd in samenhang met de nieuwe middelen en methodes van kennisverwerving. En met de karakterverandering van kennis verandert ook de politiek van kennis.

Wie is de 'eigenaar' van de verworven kennis van en over individuele burgers of groepen van burgers? En wie verwerft kennis? Verschillende auteurs wijzen erop dat kennis en toezicht tweerichtingsverkeer zijn. De burger kijkt terug en heeft zijn eigen visie. Politiek gevolg van de veranderende technieken van toezicht is ook dat de openbare ruimte niet meer

dezelfde is, of algemener gesteld, dat de sfeer van de openbaarheid niet meer dezelfde is. Volgens de ene auteur alles zichtbaar gesteld, openbaar, volgens de andere is de openbaarheid alomtegenwoordig en daarom eigenlijk verdwenen. Wat betekent transparantie dan?

Een terugkerend thema in verschillende bijdragen is dat toezicht niet neutraal is: toezicht veronderstelt dat er iets gezien wordt en heeft in zijn door informatietechnologie bemiddelde vorm zijn uitwerking op degene die gezien of geregistreerd wordt. De verdeling van kennis en macht is ongelijk Wat zijn de (mogelijke) gevolgen van toezicht voor individuen en de maatschappij als geheel, in het bijzonder de verdeling van kennis en macht?

Toezien en toekijken

De inzet van de eerste twee hoofdstukken van dit Jaarboek is om de verandering van ruimte door toezicht te analyseren.

Ike Kamphof zoekt het verschil in de intentionaliteit van het kijken. Kijken gebeurt op een bepaalde manier en wanneer zichtbaarheid de opzet is, wordt het kijken al snel voyeurisme. De figuur van de detective symboliseert deze blik, dit kijken dat een onbeperkte toegang tot de naakte waarheid veronderstelt. Waar simpele zielen niet snappen hoe in hun midden een misdaad kan worden gepleegd, legt de detective de aanwijzingen netjes op een rij en haalt zo de objectieve geschiedenis boven tafel. Er moet dus voortdurend opgelet worden en wie kan dat beter dan een bewakingscamera? Maar wat ziet de camera? Kamphof beargumenteert dat een camera niets kan met misdaad die zich niet in de openbare ruimte afspeelt. Ook helpt een camera niet tegen misdaad die zich überhaupt niet probeert te verbergen, zoals ‘happy slapping’. Met deze twee argumenten brengt Kamphof aan het licht dat de camera allerminst een neutrale waarnemer is: ze kleurt de omgeving onvermijdelijk als onveilig.

De blik van de camera is niet als het oog van God; de camera kan niet ‘naar binnen’ kijken, naar de beweegredenen achter gedrag. De lens ziet alleen de platte bewegingen en disciplineert daarom ook dat gedrag. Wie zich in het blikveld bevindt weet dat intenties niet tellen, men wil slechts vermijden als verdacht aangemerkt te worden. De camera mist ook het zorgende aspect van het oog van God. De blik van de camera is alleen gericht op het constateren van afwijkingen, niet op het geven van aandacht. Zo laten ouders hun kinderen bewaken door een camera, zodat ze op dat moment niet voor ze hoeven te zorgen. Noodzakelijk is het niet dat de camera met zo’n niet-ziende, niet-zorgende blik wordt ingezet. Kunst is een van de manieren om de intentionaliteit van de camera anders te zien. Verschillende kunstprojecten tonen dat camera’s meer kunnen zijn dan toezicht, dat ze een wezenlijke rol kunnen hebben, ook in een zorgende mens-wereld relatie.

Wim Nijenhuis beschrijft de ontwikkeling van de relatie tussen het zelf en de omgeving vanuit de veranderingen in toezicht en transparantie. Door verschuivingen in tijd (informatie kan real-time worden weergegeven) en ruimte (de omgeving wordt een interactieve virtualiteit) verandert onze relatie tot de wereld. De toenemende transparantie verandert de contouren van de politiek, want de openbaarheid heeft niet langer een aparte plaats, ze is alomtegenwoordig. Het gevolg is dat een politiek van de ruimte plaatsmaakt voor een politiek van de tijd. Ook hier is het real-time aspect essentieel. De mens hoeft zich niet langer te verplaatsen om deel te nemen aan en onderdeel te zijn van de wereld, de mens zit. Controle kan nu twee dingen betekenen: toezicht op en beschikking over de omgeving.

Met de veranderingen in vormen en technieken van toezicht, verandert ook het beoordelingskader. Was privacy voorheen een onaantastbaar principe, het lijkt nu een domein van onderhandeling te zijn. Privacy, het recht om met rust gelaten te worden, stelde

natuurlijke grenzen aan de nieuwsgierigheid van de buren en het toezicht van de overheid. In zijn ode brengt Gerard Alberts de verzetsstrijdster en advocate Lau Mazirel in herinnering als een van hoeders van dit principe. Was er in 1970 nog grootschalig verzet tegen de volkstelling, in de eenentwintigste eeuw is met DNA-tests, Bonuskaarten, het Big Brother televisieprogramma en Facebook het begrip van binnenuit gerelativeerd. Persoonsgegevens zijn een ruilmiddel geworden; privacy een kwestie van onderhandeling. Om de verandering te begrijpen volstaat het niet de denkbeelden van privacy en autonomie in herinnering te roepen, men moet ook onder ogen zien dat de beoordeling niet een afweging kan zijn van voors en tegens maar vraagt naar principes: geen gevolgenethiek, maar een principe-ethiek.

Zorg en handhaving

Bijna dagelijks verschijnt er nieuwe technologie voor toezicht, opsporing en handhaving op de markt. Every breath you take (ademanalyse), every move you make (bewegingsdetectie), every step you take (camera's), alles kunnen wij ermee in de gaten houden. Maar waartoe, waarom en met welke bevoegdheid? Die en andere vragen moeten wetenschappers zich meer stellen, stelt Bob Hoogenboom in zijn column 'De maximaal beveiligde samenleving en nieuwe surveillancetechnieken'.

Hoogenboom wordt op zijn wenken bediend. Esther Keymolen en Dennis Broeders doen verslag van hun onderzoek naar de mogelijkheden van de digitale toezichtsystemen voor de jeugdzorg. Opgeschrikt door enkele nare voorvallen ziet deze sector zich genoodzaakt om meer systeem aan te brengen in het inzicht in de problemen van jeugdigen en hun omgeving, maar ook in het toezicht op de jeugdigen en op de bemoeienis van professionele hulpverleners. Het blijkt lastig te zijn om grip te krijgen op de verschillende systemen voor de jeugdzorg, de niveaus daarin, de uiteenlopende mogelijkheden, de gevolgen en de resultaten. De jeugdzorgsystemen blijken van alles te kunnen automatiseren, zelfs de beslissing welke instantie waarvoor verantwoordelijk is. Dat roept de vraag op of de beslissingen en de afwegingen wel de maat houden van de problematiek van de jeugdige. En hoe zit het met de kwaliteit van het toezicht op de kennis in deze systemen? De jeugdige ontvangt niet van alle registraties in het systeem bericht. Gaan jeugdzorginstellingen zich niet verschuilen achter deze niet-zichtbare registraties, en zich daarmee onttrekken aan het toezicht dat transparantie heet?

Function creep, zo noemt men de onbedoelde functieverschuiving van techniek. De telefoon werd misschien ontwikkeld voor zakelijk bankverkeer, het grote succes dankt deze techniek aan de communicatie in de privésfeer. In het geval van het digitale controlesystemen houdt function creep volgens Peter Marks, Arie van Sluis en Victor Bekkers een maatschappelijk risico in. Grootschalige toepassing van systemen ter verzameling van informatie over goederenstromen werd oorspronkelijk bepleit ten behoeve van veiligheid (terreurbestrijding en bestrijding van de georganiseerde criminaliteit). Nu deze systemen gerealiseerd zijn, leveren ze spanningen op met vrijheid en grondrechten, met doelmatigheid en met gelijkheid. De veelheid aan observatiemiddelen en databestanden en het gebrek aan toezicht daarop kunnen een bedreiging vormen voor de grondrechten van personen. De ongebreidelde groei en toepassing van alles wat mogelijk is aan en in controlesystemen brengen hoge kosten met zich mee. Wanneer dan de kosten ertoe leiden dat de goederenstromen zich verplaatsen naar locaties met lage kosten, levert dat weer een bedreiging op voor de veiligheid. Dan is de doelmatigheid uit het zicht verdwenen. De keuze waar wel en waar geen informatie te verzamelen levert bovendien rechtsongelijkheid tussen personen, tussen groepen en organisaties.

Data mining en spiegelwerelden

Eén van de belangrijkste gangmakers van het toenemend toezicht is de informatietechnologie. De toenemende opslag- en verwerkingscapaciteit maken het verzamelen en bewaren van gegevens en verbanden daartussen steeds gemakkelijker.

Irma van der Ploeg problematiseert in haar essay de relatie tussen toezicht en kennis in de hedendaagse surveillance studies. Zij richt zich in het bijzonder op het gebruik van databanken, verzamelen van persoonsgegevens en *profiling*, die zij schaart onder het begrip data mining. Data mining behelst niet alleen het verzamelen van kennis, maar vooral het genereren van nieuwe kennis door koppeling van bestanden. Kennis is daarbij zowel output (wat levert de data mining op) als input (waarbij de vraag is welke kennis wordt verzameld en opgeslagen). Aan de hand van voorbeelden van databanken laat Van der Ploeg zien dat persoonlijke gegevens die worden geregistreerd, verspreid raken over gedistribueerde kennissystemen en vervolgens vrijwel onmogelijk kunnen worden gewist. De geregistreerde personen lopen als het ware een parallelle, digitale identiteit op. Er ontstaat een nieuwe manier van kennisproductie die gebaseerd is op automatische, snelle en continue analyse van geregistreerde handelingen, bewegingen en uitingen van mensen. Dat er informatie van en over burgers wordt opgeslagen en verwerkt is niet nieuw, het automatisch genereren van statistische verbanden en patroonherkenning is dat wel. Correlaties worden niet gevonden op basis van een vermoeden, maar omdat de datasets de verbanden zelf aangeven (in de literatuur staat dat bekend onder de noemer intelligence-led policing[2]).

Om deze ontwikkeling te begrijpen moeten we volgens Van der Ploeg goed kijken naar de wijze waarop input wordt gegenereerd. Vaak nemen de registraties het lichaam als uitgangspunt (identificerende biometrische kenmerken, maar ook informatie over lichaamshouding verkregen via camera's en sensoren). Het classificeren van normaal en afwijkend gedrag wordt vervolgens gebruikt om preventief op te treden. Als het gaat om gebruik van ICT, dan wordt de gebruiker gedefinieerd als degene die de data mining gebruikt en niet degene van wie de digitale identiteit is gegenereerd. Dit creëert een kennisasymmetrie die groter is dan in de klassieke surveillance. De kennis gaat over het gedrag van mensen en de voorspellers daarvan die in surveillance systemen zijn ingebouwd. Vaak wordt daarbij uitgegaan van vaste kaders en wetmatigheden. De voorspellende modellen leggen bijvoorbeeld verband tussen etniciteit en ongewenste activiteiten. Meer en meer verdwijnt de mens uit deze 'vertaalslag' door computergestuurde analyses. Dit maakt analyses weliswaar overzichtelijker en minder tijdrovend, maar roept wel ethische vragen op. Van der Ploeg pleit voor een multidisciplinaire onderzoeksaanpak om deze ontwikkelingen te doorgronden.

Rinie van Est, Floortje Daemen en Christian van 't Hof beschouwen in hun bijdrage een specifieke technologie, Google Earth. Ze stellen dat met de technologie waarin informatie op kaarten is geïntegreerd een digitale spiegelwereld wordt gecreëerd, waardoor we ons steeds meer 'in' het net bevinden in plaats van erop. De tendens is dat de spiegelwereld steeds meer real-time wordt. Informatie over de positie van vrienden kan gevolgd worden; met behulp van de camera van de mobiele telefoon kan informatie over de omgeving opgevraagd worden. Nu al zien we toevallige voorbijgangers in Street View, maar waarom dan niet ook meteen live-beelden van (bewakings)camera's integreren?

Deze ontwikkeling heeft mogelijk gevolgen voor nationale veiligheid, empowerment en commercialisering. Aan de ene kant biedt het platform allerlei mogelijkheden voor burgers om hun leven vorm te geven, maar welke mogelijkheden zijn er nog om een privé-omgeving beschermen wanneer alles vastgelegd wordt? En hoe maakt men het onderscheid tussen politiek neutrale informatie en het business-model van Google dat erachter zit, en dat uiteindelijk draait om het verkopen van advertenties?

Voorzorg en LAT-relaties

De burger kijkt terug. Martijn Stevens laat zien dat het gebruik van digitale media en mobiele technologie niet alleen nieuwe mogelijkheden biedt voor commerciële partijen of de overheid, maar ook voor de burger zelf. Het opnemen van rellen bij een strandfeest door aanwezigen leidt tot nieuwe vormen van toezicht *door de burger zelf*, zogeheten 'sousveillance' of 'participatief panoptisicme'. Zulke middelen worden bijvoorbeeld ook ingezet bij politieke onrust (bijvoorbeeld in Iran), of bij grootschalige rampen (de orkaan Katrina, de aardbeving in Haïti, de olieramp Golf van Mexico). Daarmee vormen zij een middel voor de burgers om de overheid of private organisaties van informatie te voorzien, maar deze daarmee tegelijkertijd juist ook onder druk te zetten.

Charlotte van Ooijen en Stefan Soeparman beschrijven twee tegengestelde discoursen over de nieuwe vormen van overheidstoezicht.

In het eerste discours staat de controle van de staat centraal. Dit discours rondom de controlestaat is terug te voeren op Foucaults interpretatie van Benthams panopticon. 'Big brother is watching you' is een typische uitdrukking die bij het discours van de controlestaat hoort. De (achterhaalde maar nog steeds levende) uitdrukking is ter waarschuwing voor een totalitaire staat die de gedragingen van haar burgers controleert en (onzichtbaar) stuurt. Kennis over (het gedrag van) de burger is voor de overheid cruciaal in de controlestaat. De staat bekijkt de burgers, niet andersom. Omdat kennis asymmetrisch is verdeeld, functioneert kennis als machtsbron voor de overheid. Het gebruik van ICT hulpmiddelen stelt de overheid in staat een 'superpanopticon' te bouwen. Niet langer is er een wachttoren maar zijn er meerdere, met elkaar in verbinding gebracht door ICT.

In het tweede discours is de overheid afzijdig of gedraagt zich als partner van de burger. De sociale staat past binnen dit discours. In deze staat is de burger sociaal-expressief en kan zij invloed uitoefenen op de activiteiten van de staat, zeker als zij gebruik maakt van nieuwe ICT-mogelijkheden zoals social networking sites (weblogs, twitter, etc.). Naast negatieve consequenties van de nieuwe ICT, krijgt zelfcorrigerend vermogen op deze wijze een kans. De burger geeft (vrijwillig en vaak onbewust) wel veel van haar eigen privacy weg.

Volgens de auteurs schieten beide discoursen tekort om een evenwichtig beeld te schetsen van de wijze waarop burgers en overheid met elkaar in contact staan en kennis over elkaar genereren. Daarom komen ze met een alternatief, derde discours: de voorzorgstaat. In de voorzorgstaat bestaat ook kennisasymmetrie, maar die bestaat tussen deskundigen op een bepaald gebied en burgers die van die diensten gebruik kunnen maken. Bovendien wordt de kennisasymmetrie 'aangevuld' met professionele of persoonlijke verantwoordelijkheid van de experts. De burger vraagt daar ook om: integriteit en geloofwaardigheid zijn cruciaal. Het derde discours voorkomt dat we ons blind staren op een machtsbeluste overheid met gevaar voor privacy aan de ene kant en op ongebreidelde democratische mogelijkheden van de hedendaagse kennisdeling aan de andere.

Judith van Erp en Albert Meijer leggen in hun bijdrage een verband tussen overheids- en burgertoezicht. Vanuit een aantal praktijkstudies laten ze zien dat de moderne toezichthouder niet alleen de resultaten van het toezicht deelt met het publiek, maar dat die toezichthouder de consument ziet als mede-toezichthouder. Burgers op hun beurt maken niet alleen gebruik van informatie van toezichthouders, maar kunnen hier zelf ook informatie aan toevoegen. Van Erp en Meijer spreken dan over toezicht 2.0. Met andere woorden, overheid en toezichthouders hebben niet (langer) het monopolie op informatieverstrekking aan burgers. Een probleem bij burgertoezicht is dat het wordt uitgevoerd door ongetrainde leken. De kwaliteit van de geleverde informatie is dan een probleem. Veel centrale toezichthouders zien

toezicht 2.0 dan ook eerder als ruis, dan als een welkome aanvulling op de informatievoorziening. Vooralsnog staat de 2.0 cultuur te ver af van de vaak bureaucratische overwegingen van toezichthouders.

De toegenomen verstrengeling van toezichthouders en burgers verklaren de auteurs uit drie ontwikkelingen. In de eerste plaats is er de roep om een transparante overheid, die de toezichthouder dwingt informatie van en over burgers transparant te maken. In de tweede plaats is de samenleving veranderd, mede onder invloed van nieuwe technologie en media. De huidige samenleving laat zich het best omschrijven als een globale netwerksamenleving waarin het morele gezag van toezichthouders niet vanzelfsprekend is. Effectief toezicht in deze samenleving gaat om het handig inspelen op het krachtenveld van wat de auteurs 'controlerende actoren' noemen. Als derde ontwikkeling noemen Van Erp en Meijer het zelforganiserend vermogen van de samenleving door middel van het Internet. Burgers kunnen op het Internet allerlei informatie vinden over zaken waar traditioneel de toezichthouder zeggenschap over had.

De invloed van de informatie van de toezichthouder op het uiteindelijke gedrag van de burger – die eigenlijk consument is geworden – wordt overschat. Veel analyses van toezichthouders gaan uit van de burger als rationele beslisser. In werkelijkheid echter, laten burgers zich niet alleen door rationele overwegingen leiden. Bovendien sluit lang niet alle informatie van de toezichthouder aan bij de informatiebehoefte van burger en consument.

Van Erp en Meijer pleiten voor een synergie, maar op de vraag hoe toezichthouders en burgers kunnen samenwerken, is vooralsnog geen eenduidig antwoord te geven. De auteurs laten zien dat een 'LAT-relatie' kans heeft en dat daarbij vragen als: 'Zijn opvattingen over kwaliteit van informatie aanvullend?', 'Welke eisen worden gesteld aan de kwaliteitsoordelen?' en 'Wordt er op dezelfde doelgroepen gemikt?' mede kunnen bepalen of het inderdaad nuttig is informatie van de toezichthouder en informatie uit burgerinitiatief te koppelen.

Het toezien van 2010

Uit de artikelen van dit Jaarboek blijkt dat anno 2010 de idee van een Big Brother-samenleving achterhaald is. De vormen van toezicht die door nieuwe technologie mogelijk worden gemaakt, blijken niet alleen betrekking te hebben op het politieke discours van veiligheid en controle. Naast veiligheid is ook de verzorgingsstaat een belangrijke drijfveer voor meer toezicht, zoals in patiëntendossiers, kinddossiers en registraties van hulpverlening aan probleemjongeren. Dit toezicht door de overheid is echter niet eenzijdig: de technologie leidt vooral ook tot nieuwe mogelijkheden voor de burger, waarbij ook toezichthouders constant onderwerp van controle lijken te worden. Big Brother wordt zo meer een Soft Sister.[3]

De voorzorgstaat is geopperd als middel om alle nieuwe mogelijkheden binnen een maatschappelijk discours vorm te geven. Dit lijkt een soort vertaling te zijn van het voorzorgsbeginsel - bekend uit de milieu- en gezondheidsethiek - naar de informatietechnologie.[4] Hierbij wordt een discussie beoogd waarin verschillende belanghebbenden, inclusief experts, de mogelijke gevolgen van technologische ontwikkelingen in kaart brengen, en met methoden als value-sensitive design bij voorbaat al ongewenste ontwikkelingen zoals function creep zo veel mogelijk uitsluiten.[5]

Het sturen van de ontwikkeling van toezicht in een kennissamenleving is geen eenvoudige opgave. Niet alleen is er politieke discussie, ook zijn er spontane ontwikkelingen die zich grotendeels aan sturing onttrekken, en deze zullen in Web 2.0 omgevingen alleen maar sterker worden. De vormen van kennis waarop het toezicht is gebaseerd, zullen steeds

ter discussie blijven staan, of deze nu verankerd zijn in overheid, wetenschap, of burgerparticipatie. Bovenal blijkt dat toezicht een reflexief begrip is. Om toezicht goed te organiseren zal ook op de middelen die daarvoor worden ingezet een bepaalde vorm van toezicht nodig zijn. Daarvoor is niet alleen kennis nodig, maar vooral ook inzicht.

Literatuur

Friedman, B., Kahn Jr, P.H. & Borning, A. (2006). Value Sensitive Design and information systems. In: P. Zhang & Galletta, D. (Eds.) *Human-Computer Interaction and Management Information Systems: Foundations*: 348-372. New York: ME Sharpe.

Jacobs, B.P.F. (2007). *De menselijke maat in ICT*. Online boek, http://www.cs.ru.nl/B.Jacobs/MM/, ISBN 978-90-9021619-5.

Pieters, W. and van Cleeff, A. (2009). The Precautionary Principle in a World of Digital Dependencies. *IEEE Computer*, 42(6), 50-56.

Ratcliffe, J.H. (2008). *Intelligence-Led Policing*. Cullompton: Willan Publishing.

Wagenaar, P. & Boersma, F.K. (2008). Soft sister and the rationalization of the world. The driving forces behind increased surveillance. *Administrative Theory & Practice*, 30(2), 184-206.

[1] Jacobs (2007).
[2] Ratfliffe (2008).
[3] Wagenaar en Boersma (2008).
[4] Pieters en Van Cleeff (2009).
[5] Friedman, Kahn Jr en Borning (2006).