

Toezichttechnologie en recht: ingrijpende maatschappelijke consequenties zijn voorspelbaar*

Pieter Kleve, Richard De Mulder en Kees van Noortwijk

Abstract

In this article, attention will first be paid briefly to supervision technology as such. An attempt will be made to sketch out the extent and the limitations of the techniques. A question then addressed is why the use of supervisory technology is growing. Given the increasing interest in supervision technology, an examination is made of the permissibility of the use of this technology taking certain constitutional and legal rights into account. What is the role of supervisory technology within the context of wider social developments? The article reaches the conclusion that with the increasing significance of supervision technology and the increasing use of it the importance of 'supervision of the supervisors' will increase as well.

Samenvatting

In dit artikel wordt eerst summier ingegaan op toezichttechnologie als zodanig. Beoogd wordt een beeld te scheppen van de reikwijdte en de beperkingen van de technieken. Tevens wordt getracht inzicht te geven in de oorzaken van het toenemende gebruik van toezichttechnologie. Vervolgens wordt ingegaan op de vraag naar de toelaatbaarheid van het gebruik van technologie voor toezichtdoeleinden in het licht van enkele van belang lijkende grondrechten en rechtsbeginselen. Daartoe wordt het gebruik van toezichttechnologie eerst binnen een bredere context van maatschappelijke ontwikkelingen geplaatst. Het artikel besluit met de conclusie dat met de toenemende significantie van toezichttechnologie en het toenemend gebruik ervan ook het 'toezicht op de toezichthouders' in belang zal toenemen.

1. Inleiding

Dinsdag 30 augustus 2005 ontvingen circa 17.000 mobiele-telefoongebruikers die zich blijkens de zendmastgegevens van de telefonie-providers tijdens de voetbalrellen van 17 april 2005 in de nabijheid van voetbalstadion 'De Kuip' bevonden een SMS van de politie uit Rotterdam, met het verzoek om medewerking te verlenen aan het onderzoek dat naar de rellen is ingesteld. Dit is een van de vele voorbeelden waarin recente technologie wordt gebruikt voor het uitoefenen van toezicht. Dergelijk gebruik van technologie ontmoet vaak kritiek vanuit de samenleving vanwege mogelijke inbreuken op het recht op bescherming van de persoonlijke levenssfeer, met name in verband met het '*big brother*'-gevoel dat daarbij ontstaat.¹

* In: Rogier, L.J.J. en H. de Doelder, (Eds.), *Toezicht: opstellen over veiligheidstoezicht en markttoezicht*, p. 211-236, Boom Juridische uitgevers: Den Haag, 2005.

¹ In plaats van 'Big Brother' uit George Orwell's *Nineteen Eighty-Four* als metafoer, waarin inbreuk op privacy bestaat uit het uitoefenen van toezicht, en schade uit een gevoel van schaamte, verlies van reputatie, zelfcensuur en beperking, kiest Solove voor de bureaucratie uit Kafka's *Het Proces*. Het probleem is machteloosheid, kwetsbaarheid en 'ontmenselijking', als gevolg van de aanleg van dossiers met persoonlijke informatie buiten betrokkenen om en zonder dat zij invloed hebben op het

Technologie voor toezicht is in de hedendaagse maatschappij al een heel gewoon verschijnsel. Voorbeelden zijn gemakkelijk te vinden.

- Omdat luchtverontreiniging een risico is voor de volksgezondheid, staan in het Rijnmondgebied bij Rotterdam zogenoemde ‘snuffelpalen’ waarmee de luchtverontreiniging wordt gemeten. Wanneer de verontreiniging boven zekere waarden uitkomt, wordt een waarschuwingssysteem geactiveerd.
- Naar aanleiding van de desastreuze gevolgen van de tsunami in december 2004 wordt er een tsunami-waarschuwingssysteem aangelegd in de Indische Oceaan.²
- In fabrieken en in de industrie worden talloze processen ‘gemonitord’ met behulp van technologie. In ziekenhuizen worden processen in het menselijk lichaam gemonitord. En ons betalingsgedrag wordt gemonitord door computers, die ons een aanmaning sturen wanneer de betalingstermijn is verstreken.

Toezichttechnologie is de orde van de dag, overal in de wereld. Technologie wordt gebruikt voor toezicht op de werking van maatschappelijke en fysieke processen, voor toezicht op de werking van lichamelijke processen en voor toezicht op individueel gedrag.

O.a. omdat hard rijden een risico is voor de volksgezondheid staan er in het gehele land zogenoemde ‘flitspalen’, waarmee de snelheid van voertuigen wordt gemeten. Wanneer een snelheid boven een bepaalde waarde wordt gemeten, wordt er een foto van het voertuig gemaakt en de gemeten snelheid vastgelegd, waarna de aanschrijving tot het betalen van een administratieve boete uitgaat. Dit ‘flitsen’ geschiedt slechts in reactie op een overtreding op de plaats van de flitspaal. Een overtreding juist voor of enige tijd na het bereiken van de flitspaal leidt niet tot een bekeuring. Een nieuwe ontwikkeling is dan ook trajectcontrole. Een camera registreert het langskomen van een voertuig alsmede de tijd waarop dit geschiedt. Kilometers verderop registreert een tweede camera dezelfde gegevens en een computer berekent de gemiddelde snelheid over het afgelegde traject. Als die gemiddelde snelheid te hoog is, verzorgt het systeem weer de bekeuring. Het rijgedrag aanpassen voor de duur van het maken van een foto is niet langer toereikend, men zal zich nu gedurende het gehele traject moeten inhouden. (Anderzijds evenwel, leidt een kortstondige overtreding van de maximumsnelheid gedurende het traject niet tot bekeuring.)

Door toepassing van technologie is er sprake van een toenemende conditionering van gedrag. De legitimatie van die conditionering vindt (in het hiervoor besproken geval) zijn grond in de situatie dat daar een rechtmatig besluit tot vaststelling van maximum snelheden aan vooraf is gegaan, en dat de uitvoering aan rechtstatelijke controle onderhevig is. Toch blijkt dat, hoewel we aan het gebruik van flitspalen wel gewend zijn geraakt, de toepassing bij sommigen nog veel agressie oproept. Wellicht is het zo, dat we zelf het overschrijden van de maximum snelheid niet zo erg vinden, of dat we er een goede reden voor menen te hebben (die de rechter helaas niet zal honoreren).

gebruik daarvan. D.J. Solove, ‘Privacy and Power: Computer Databases and Metaphors for Information Privacy’, *Stanford Law Review*, 2001 Vol. 53, <http://docs.law.gwu.edu/facweb/dsolove/Privacy-Power.pdf>. Vgl. ook de conclusies uit het eindrapport van de Commissie Koopmans (T. Koopmans (voorz.), *Privacy en persoonsregistratie*, Sdu 1976).

² Eerder is in de Stille Oceaan een tsunami-waarschuwingssysteem aangelegd, nadat in 1946 een aardbeving bij Alaska een tsunami veroorzaakte met ruim 150 dodelijke slachtoffers, merendeels in Hawaii.

Bij controle en aanhouding door een agent – kan men denken – kon je nog wel eens wegekomen met een goed verhaal.

In reactie op de plaatsing van flitspalen zijn er automobilisten die hun toevlucht nemen tot radardetectieapparaten, opdat ze worden gewaarschuwd wanneer ze een radargecontroleerde snelheidsmeting naderen. En in reactie daarop zijn er dan weer overheidsfunctionarissen die radardetectieapparaten willen verbieden. (En daar weer in reactie op zijn er fabrikanten die radardetectieapparaten aanbieden die buiten de categorie van ‘illegale radardetectieapparaten’ vallen.)³ Wat opvalt is, dat een rechtsregel niet zonder meer tot naleving aanzet, maar een aaneenschakeling van gedragingen tot gevolg heeft van individuen die steeds hun eigen belang nastreven. Zo’n ‘kettingreactie’ doet ook de aandacht vestigen op de relatie tussen rechtsregel en handhaving. De handhaafbaarheid van een rechtsregel is een belangrijk aspect. Gebruik van technologie kan de handhaving of naleving bevorderen, zij het dat dat niet altijd of zonder meer het geval hoeft te zijn.

Cameratoezicht vindt men niet alleen in het verkeer. Tegenwoordig is het gebruik van camera’s gemeengoed in winkels, bij benzinepompen en op industriegebieden, bijvoorbeeld. En het cameratoezicht rukt alsmat op. In particuliere woningen, bij geldautomaten en gewoon op straat staan steeds vaker camera’s. En nog onlangs werd het plan gelanceerd het cameratoezicht reeds op de toegangswegen naar de stad te laten beginnen. De hoofdcommissaris van de Amsterdamse politie sprak in dit verband over een ‘virtuele slotgracht’.

Wat al geen plan meer is, maar praktijk, is de toegangscontrole (en vertrekcontrole) die de Verenigde Staten van Amerika hanteren voor buitenlanders. Wie de V.S. binnen wil, dient van beide wijsvingers vingerafdrukken te laten nemen, te completeren met een pasfoto. De persoonsgegevens zijn al door de vliegmaatschappij verstrekt. Eenmaal op bezoek bij de zakelijke relatie blijkt dat het vertrouwde ‘gastenboek’ is ingeruild voor een videoregistratie met het vriendelijke verzoek even in de camera te kijken en de naam te zeggen.

Het gebruik van camera’s is wellicht het meest voor de hand liggende voorbeeld waarbij men het gevoel krijgt ‘bekeken te worden’, maar er zijn inmiddels andere technologische ontwikkelingen die even ingrijpend, zomet ingrijpender zijn. ‘Internetten’ bijvoorbeeld blijkt niet zo anoniem als voorheen wel werd verondersteld. Al surfend op de digitale snelweg laat men talloze sporen achter die dankbaar worden getraceerd door bedrijven die internetgedrag in kaart willen brengen. Gelet op het staatsmonopolie op de toepassing van dwangmiddelen is het voor de overheid zelfs nog eenvoudiger toegang te verkrijgen tot deze ‘sporen’. Opwinding ontstond er evenwel na de onthulling in de pers van het omstreden Echelon-programma van de Amerikaanse National Security Agency (NSA), dat wereldomspannend toezicht op

³ Zie bijvoorbeeld ook art. 32a Auteurswet 1912, waarmee het kraken van technische beveiligingen bestreden moet worden. Deze bepaling illustreert eveneens dit merkwaardige proces van ‘stapeling’, indien men bedenkt dat het auteursrecht een middel is, tegen het onbevoegd kopiëren van oorspronkelijke werken, dat dit juridische middel kennelijk ontoereikend is waarop de industrie besluit tot technische voorzieningen ter bescherming van werken, dat technische middelen kennelijk ook niet toereikend zijn, waarop wordt teruggegrepen naar juridische bescherming, maar nu van de technische bescherming. De lamme helpt de blinde.

(of ‘af luisteren’ van) de data-uitwisseling op het internet omvat.⁴ Anderzijds kan men zich afvragen of er niet een grotere mate van opwinding zou ontstaan, indien zou blijken dat de NSA dat níet zou doen.⁵

2. Toezicht met behulp van technologische hulpmiddelen

Uit de gegeven voorbeelden blijkt reeds dat technologie een belangrijke, in bepaalde gevallen zelfs essentiële rol kan vervullen bij het uitoefenen van toezicht. Daarom zal nu worden stilgestaan bij een reeks van mogelijkheden voor toezicht welke met IT-hulpmiddelen kunnen worden gerealiseerd. Het toezicht is in dat verband niet uitsluitend gericht op de naleving van het bepaalde bij of krachtens enig wettelijke voorschrift.⁶ Toezicht door overheidsinstanties vormt in veel gevallen het beginpunt van een keten waartoe verder ook de opsporing en de vervolging behoren. Ook bij deze vervolgschakels vormt IT tegenwoordig een niet meer weg te denken hulpmiddel.⁷

Centraal staat hierbij de informatietechnologie of IT. Vaak wordt hiervoor ook de term ICT, Informatie- en *Communicatie*Technologie, gebruik. Communicatietechnologie is echter een vast en essentieel onderdeel van de informatietechnologie geworden, zodat het in feite niet langer noodzakelijk is er afzonderlijk melding van te maken. Dat geldt ook voor andere componenten van de IT, we spreken immers evenmin van ‘informatie- en dataopslag-technologie’.

2.1 Cameratoezicht in openbare en niet-openbare ruimten

Een toepassing van technologie die wellicht het nauwst verbonden is met de (algemene) toezichtsfunctie is het gebruik van audiovisuele apparatuur (camera’s) waarmee van afstand, ‘in real time’ of achteraf, een bepaalde ruimte of een bepaald gebied in de gaten kan worden gehouden. Recentelijk is overigens betoogd dat de effectiviteit van cameratoezicht in openbare ruimten aanmerkelijk hoger is bij real time observatie, met name aangezien dan direct kan worden gereageerd op waargenomen feiten.⁸

Voor zover het toezicht ‘in real time’ betreft is de rol van IT wellicht niet direct helder: het gaat in principe om een camera verbonden met een monitor waarachter

⁴ Het Amerikaanse FBI werkte met een eigen systeem, Carnivore, voor het ‘af luisteren’ van email en internetverkeer. Inmiddels is de strategie gewijzigd en maakt men meer gebruik van standaard commerciële programma’s en richt men zich meer rechtstreeks tot de internetproviders.

⁵ In de USA Patriot Act 2001 (Pub. L. No. 107-56, 115 Stat. 272), antiterrorismewetgeving die versneld tot stand kwam in reactie op de aanslagen van 9 november 2001, heeft het Congres de werkingsduur van enkele belangrijke bevoegdheden met betrekking tot elektronisch toezicht op het internet vanwege het (verondersteld) verstrekkende karakter begrensd tot 31 december 2005. Volgens Kerr brengt de USA Patriot Act 2001 nauwelijks uitbreidingen op het gebied van de handhaving, maar is de wet vooral een hercodificatie van reeds bestaande wetten. O.S. Kerr, ‘Internet Surveillance Law After the USA Patriot Act: The Big Brother That Isn’t’, *Northwestern University Law Review*, Vol. 97, 2003, <http://ssrn.com/abstract=317501>.

⁶ Vgl. artikel 5:11 Algemene wet bestuursrecht,

⁷ Zie voor een overzicht van IT-toepassingen in het kader van veiligheid R.V. De Mulder, K.H. Oey en P.C. van Schelven, ‘Veiligheid en IT, IT en veiligheid’, in: Muller, E.R. (Ed.), *Veiligheid: studies over inhoud, organisatie en maatregelen*, p. 711-740, Alphen aan den Rijn: Kluwer 2004.

⁸ B. Bieleman & J. Snippe, ‘Mensenwerk, voorwaarden voor succesvol cameratoezicht’, in: *Secondant #5/2005*, oktober 2005, p. 26-31.

zich een menselijke toezichthouder bevindt. Het videosignaal wordt tegenwoordig echter dikwijls niet meer in analoge vorm opgenomen en verzonden, maar wordt direct gedigitaliseerd. Dat opent diverse nieuwe mogelijkheden.

Om te beginnen kunnen de videobeelden veel gemakkelijker naar verschillende locaties worden verzonden. Dat is met name het geval wanneer de camera voorzien is van een netwerkaansluiting en kan communiceren via het internetprotocol. De beelden kunnen dan in principe op iedere computer verbonden met het internet worden bekeken.

Dat bekijken van beeldmateriaal kan daarbij op de traditionele manier gebeuren, waarbij de waarnemer kan schakelen tussen de signalen van verschillende camera's of desnoods de beelden van die camera's naast elkaar op het scherm kan laten projecteren. Elektronische beeldverwerking, waarbij een computer het materiaal op verschillende niveaus kan analyseren en bewerken, behoort tegenwoordig echter ook tot de mogelijkheden. Te denken valt daarbij bijvoorbeeld aan de volgende technieken (min of meer in volgorde van oplopende complexiteit):

- Motion detection of soortgelijke technieken die ervoor zorgen dat alleen opnamen worden getoond of bewaard waarin ook echt iets gebeurt (bijvoorbeeld in de vorm van beweging of geluid).
- Het verhogen van de scherpte, het contrast e.d. van een opname, zodat bepaalde details (een kentekenplaat, het gezicht van een persoon) beter zichtbaar worden.
- Gelaatsherkenning, de identificatie van een persoon aan de hand van een opname van zijn gelaat. Bij het verwerken en toepassen van deze vorm van biometrische informatie (waarover later meer) is de laatste jaren grote vooruitgang geboekt. De toepassing wordt in het rapport van de commissie Criminaliteit en Technologie⁹ een van de "meest veelbelovende" technieken genoemd. Het is thans al mogelijk om met deze techniek personen te identificeren die zich in een menigte bevinden (mits vanzelfsprekend het gelaat van de persoon in kwestie op enig moment zichtbaar is). De toepassing van de techniek wordt als relatief laagdrempelig gezien, het maken van een opname van het gezicht wordt als minder bedreigend gezien dan bijvoorbeeld het maken van een irisscan. Er wordt dan ook al geëxperimenteerd met toegangscontrole gebaseerd op deze techniek (soms in combinatie met bijvoorbeeld vingerafdruk-scanning) bij kantoorgebouwen, maar ook bij ziekenhuizen en zelfs bij zwembaden.¹⁰
- Wanneer camerabeelden van verschillende locaties ter beschikking staan: 'tracking and tracing' van personen op basis van gelaatsherkenning. Door middel van deze techniek wordt in detail bijgehouden waar een persoon zich wanneer bevindt waaruit kan worden afgeleid welke route deze (bij benadering) aflegt.
- Patroonherkenning ('Object Pattern Analysis'). Hierbij worden beelden vergeleken waarbij alleen gebeurtenissen die er op welke manier ook uitspringen worden gemeld of geregistreerd. Het is op dit moment al mogelijk om met deze techniek personen die zich afwijkend gedragen (bijvoorbeeld zich veel langer dan gemiddeld op een bepaalde plaats ophouden) te onderscheiden. Ook kan de techniek worden gebruikt om afwijkende patronen m.b.t. bijvoorbeeld voertuigen

⁹ Commissie Criminaliteit en Technologie, *Technologie en Misdaad, Kansen en bedreigingen van technologie bij de beheersing van criminaliteit*, 's-Gravenhage: Ministerie van Justitie 2005

¹⁰ 'Toegang zwembad met vingerafdruk', *NRC Handelsblad* 16-08-2005, p. 2.

aan het licht te brengen, zoals personen- of vrachtauto's die een opvallend routepatroon vertonen.

- Gebruik van beeldmateriaal afkomstig van speciale satellieten, die zijn voorzien van geavanceerde camera- en sensorapparatuur waarmee personen of goederen kunnen worden gelokaliseerd, geïdentificeerd en gevolgd.

Uit het bovenstaande moge duidelijk zijn dat de 'traditionele' vormen van cameratoezicht en -beveiliging, waarbij analoog beeldmateriaal via een specifieke, afzonderlijke infrastructuur wordt getransporteerd naar een locatie waar de beelden worden bekeken of op band worden opgenomen, door de technologische ontwikkelingen zijn ingehaald. Vooral het feit dat digitale, op internettechnologie gebaseerde camera's geen afzonderlijke infrastructuur c.q. bekabeling nodig hebben is zo'n groot voordeel dat te verwachten valt dat deze techniek de analoge versie in de komende jaren geheel zal vervangen.

2.2 Toezicht op telecommunicatie

Het 'monitoren' van alle voorkomende vormen van telecommunicatie in het kader van toezicht komt – evenals het hierboven beschreven cameratoezicht – op grote schaal voor. Naast het telefoon- en faxverkeer speelt toezicht op dataverkeer (met name internet) tegenwoordig een belangrijke rol.

Technisch gesproken maakt het in veel gevallen eigenlijk niet meer uit om welk soort communicatie het gaat: ook spraakverkeer wordt in veel gevallen al direct aan de opnamekant gedigitaliseerd en pas daarna verstuurd. Dit is bijvoorbeeld het geval bij mobiele telefonie via GSM, het alomtegenwoordige 'Global System for Mobile communication' waarmee vrijwel iedere mobiele telefoon werkt. Een andere techniek waarbij spraakverkeer direct wordt gedigitaliseerd is VOIP, Voice Over IP. In dit geval wordt het audiosignaal omgezet in datapakketjes met een zodanige structuur dat ze verzonden kunnen worden via het wereldwijde internet. VOIP kan worden gebruikt tussen twee met internet verbonden computers (beide voorzien van audio-hardware), maar tegenwoordig is er ook specifieke apparatuur (in de vorm van conversiekastjes en VOIP-telefoons) die het mogelijk maakt deze techniek toe te passen zonder dat er een computer aan te pas komt. Sommigen verwachten dat deze vorm van telefonie de 'normale' telefoons binnen een aantal jaren geheel zal verdringen.

Dit alles maakt duidelijk dat het tegenwoordig weinig zinvol is bij het monitoren c.q. aftappen van datastromen al op voorhand onderscheid te maken tussen de typen communicatie die zullen worden gecontroleerd. Het is immers meestal niet mogelijk deze typen te onderscheiden zonder de gegevens eerst op te vangen en te decoderen. Dit decoderen omvat onder andere het vaststellen om welk type data (gedigitaliseerde spraak, computergegevens etc.) het gaat. Het is natuurlijk echter heel goed mogelijk dat de verzender van de gegevens een vorm van *encryptie* heeft toegepast. Dit is in principe heel eenvoudig bij digitale data. Decryptie zonder dat de toegepaste 'sleutels' beschikbaar zijn kan echter bijzonder lastig zijn en/of veel te veel tijd vergen, met name wanneer sprake is van een z.g.n. 'sterke' vorm van encryptie. Dit probleem laat zich met behulp van technologie niet een, twee drie oplossen, reden waarom van overheidswege al verschillende malen is overwogen deze encryptie aan wettelijke

regels te binden.¹¹ Zo bevatte het wetsontwerp Computercriminaliteit II aanvankelijk de bepaling dat gebruikers van encryptie in het kader van de opsporing van strafbare feiten verplicht konden worden tot decryptie van gegevens.¹² Deze bepaling is uiteindelijk echter niet in de wet terechtgekomen. Dit geldt eveneens voor een regeling om encryptiesleutels verplicht te deponeren bij ‘Trusted Third Parties’ (TTP’s).

Een specifieke vorm van toezicht, niet zozeer op het telefoonverkeer of dataverkeer zelf als wel op de personen die van (mobiele) telefoons gebruikmaken, wordt gevormd door het opvragen en benutten van locatiegegevens, dat wil zeggen gegevens afkomstig van één of meer zendmasten voor mobiele communicatie. Aan de hand van deze ‘logboekbestanden’ kan worden nagegaan wie zich op een bepaald moment op een bepaalde locatie (nl. de omgeving van deze zendmasten) bevond, wanneer de mobiele telefoon van de persoon in kwestie tenminste was ingeschakeld. Deze techniek wordt de laatste jaren al regelmatig toegepast om de gangen van een bepaalde verdachte na te gaan. De manier waarop onlangs van deze gegevens gebruik is gemaakt door de politie van Rotterdam – het versturen van sms-berichten aan alle personen die zich op een bepaald moment op een bepaalde plaats hadden bevonden – is echter nieuw voor Nederland. Het gaat daarbij dan met name om het aspect dat niet alleen gegevens van verdachten, maar van willekeurige omstanders worden gebruikt in het kader van de opsporing. Op zich nog niet eens zo spectaculair, de toepassing is door verschillende partijen al vergeleken met een traditioneel buurtonderzoek¹³, maar de schaal waarop e.e.a. is gebeurd en de overduidelijke privacyaspecten hebben toch voor de nodige commotie gezorgd.

Zowel voor dit soort ‘locatiegegevens’ als voor het dataverkeer zelf geldt vanzelfsprekend dat registratie en opslag van groot belang kunnen zijn voor toezicht achteraf. Of deze opslag het beste gerealiseerd kan worden bij de providers of op een centrale locatie en hoe lang de bewaartermijn zou moeten zijn is momenteel nog onderwerp van discussie, hoewel de minister van Justitie op dit gebied al een (voorlopig) standpunt heeft ingenomen.¹⁴ Ook op Europees niveau is regelgeving betreffende dit onderwerp in voorbereiding.¹⁵ Enig verzet hiertegen wordt geboden door o.a. de providers en organisaties die de belangen van gebruikers van het internet vertegenwoordigen zoals ‘Bits of freedom’.¹⁶

¹¹ Zie: R. van den Hoven van Genderen, ‘Het voorlopig voorontwerp tot verbod van cryptografie. De horror vacui van de ondoorbreekbare beveiliging’, *Computerrecht* 1994–4, p. 157–162. De tekst van het voorontwerp is opgenomen in *Mediaforum* 1994–6, p. B49–B55, met een inleiding van A. Patijn op p. 65.

¹² Wijziging van het Wetboek van Strafrecht, het Wetboek van Strafvordering en de Telecommunicatiewet in verband met nieuwe ontwikkelingen in de informatietechnologie (computercriminaliteit II), TK 1998–1999, 26 671.

¹³ Bijvoorbeeld P. Kleve, interview Radio Rijnmond, 31 augustus 2005 en B. Jungmann & A. Kiene, ‘Zie het als buurtonderzoek’, in: *De Volkskrant* 1 september 2005.

¹⁴ Zie de brief van de minister van Justitie aan de Tweede Kamer d.d. 5 september 2005, Kamerstukken II, 23 490, nr. 388.

¹⁵ Zie o.a. Council of the European Union, Document 12894/05 d.d. 03-10-2005: ‘Draft Framework Decision on the retention of data processed and stored in connection with the provision of publicly available electronic communications services or data on public communications networks for the purpose of investigation, detection and prosecution of crime and criminal offences including terrorism.’

¹⁶ Later in dit artikel wordt nader ingegaan op de hierbij naar voren gebracht argumenten.

2.3 Toegangscontrole, plaatsbepaling en identificatie van personen en goederen

In deze categorie valt onder andere het vaststellen van de identiteit van personen, bijvoorbeeld in het kader van toegangscontrole. Traditionele identiteitsbewijzen, voorzien van weinig meer dan een pasfoto en de naam van de persoon in kwestie, voldoen hiervoor tegenwoordig vaak niet meer, aangezien deze relatief eenvoudig te vervalsen zijn.

Een voor de hand liggende oplossing is om de vertrouwde identiteitsbewijzen – identiteitskaart, paspoort, rijbewijs – te voorzien van nieuwe kenmerken, die vervalsing bemoeilijken. Deze weg is in het verleden door de Nederlandse overheid bewandeld. Aangezien echter ook de vervalsers niet stilzaten werd op die manier in feite niet meer dan een tijdwinst van op zijn best enkele jaren gerealiseerd. Hierin kan wellicht verandering komen wanneer identiteitsbewijzen ook worden voorzien van gedigitaliseerde biometrische informatie.

Biometrie, letterlijk ‘meten van leven’, kent al een vrij lange geschiedenis. Het gebruik van vinger- en handafdrukken voor identificatie werd in China al toegepast in de 14e eeuw. In Europa worden vingerafdrukken sinds het eind van de 19e eeuw gebruikt als identificatiemiddel, volgens een systeem ontwikkeld door Scotland Yard medewerker Richard Edward Henry.¹⁷ Naast vingerafdrukken komen ook andere lichaamskenmerken in aanmerking voor identificatie, zoals de handen, de ogen (iris, netvlies), het gelaat, de stem en het DNA. Het gebruik van elk van deze kenmerken vereist specifieke technologie. De nauwkeurigheid waarmee personen eenduidig geïdentificeerd kunnen worden is bij het ene kenmerk groter dan bij het andere. In het algemeen wordt identificatie d.m.v. DNA als een van de betrouwbaarste methoden gezien. Deze methode is echter relatief tijdrovend, in tegenstelling tot bijvoorbeeld het maken van een irisscan, een gelaatsscanscan of een scan van een vingerafdruk. Deze laatste technieken zijn daardoor ook geschikt voor authenticatie in het kader van bijvoorbeeld toegangscontrole.¹⁸

Bij het gebruik van biometrische technieken speelt IT tegenwoordig meestal een belangrijke rol. Kenmerken van bijvoorbeeld een vingerafdruk worden opgeslagen in de vorm van een z.g.n. template. De nauwkeurigheid waarmee dat gebeurt bepaalt de afmetingen van de template maar ook de betrouwbaarheid ervan. Een template kan worden opgeslagen in een geheugenchip, die bijvoorbeeld kan worden verwerkt in een identiteitsbewijs.

Naast deze technieken voor identificatie van personen is een heel arsenaal aan technieken in gebruik voor het traceren en identificeren van goederen. Te denken valt hierbij aan de traditionele metaaldetectoren, bijvoorbeeld in de vorm van detectiepoorten die werken door middel van een magnetisch veld. Andere technieken die in toenemende mate worden toegepast zijn bijvoorbeeld MRI-scans, microwave radaropnamen en microwave diëlectrometrie, elk in staat om bepaalde typen stoffen in bijvoorbeeld bagage te detecteren. Explosieven kunnen onder andere worden

¹⁷ Zie A. K. Jain, L. Hong, S. Pankanti & R. Bolle, ‘An identity authentication system using fingerprints’, *Proceedings of the IEEE* 85 (9) (1997) 1365-1388.

¹⁸ De irisscan wordt hiervoor al gebruikt op de luchthaven Schiphol, de gelaats- en vingerafdrukscan door de Amerikaanse Immigration and Naturalization Service.

opgespoord met behulp van ‘Explosives Trace Detection’ (ETD), een relatief betaalbare techniek waarmee via bemonstering naar sporen van explosieve materialen wordt gezocht en met ‘Explosives Detection Systems’, kostbare automatische scanners die met behulp van röntgenstraling de inhoud van pakketten en koffers analyseren. Voor het opsporen van biologische wapens bestaan vergelijkbare technieken.¹⁹

Al deze detectietechnieken hebben gemeen dat ze gebruik maken van reeds aanwezige eigenschappen van personen of goederen. Het is echter ook mogelijk om detectie te laten plaatsvinden op basis van een speciaal voor dat doel aangebrachte markering (‘tag’). Een voor de hand liggend voorbeeld van het gebruik van deze techniek is het detectielabel dat veel winkels aan producten bevestigen en dat een alarm doet afgaan wanneer er een poortje bij de uitgang mee wordt gepasseerd. Een verwante toepassing is het verstoppertje van een tag in bijvoorbeeld een auto of scooter. Deze kan door opsporingsambtenaren met de juiste apparatuur worden uitgelezen zodat een gestolen voertuig aan de rechtmatige eigenaar kan worden terugbezorgd. Een techniek die momenteel veel in de belangstelling staat is RFID, Radio Frequency Identification. Het doel is hetzelfde als bij de veiligheidslabels, maar een RFID tag kan al bij de fabricage worden aangebracht en is zo goedkoop en klein dat in principe ieder product van dit hulpmiddel kan worden voorzien. De techniek zou daarmee mogelijk de streepjescode kunnen vervangen en tegelijkertijd ieder product effectief kunnen beveiligen tegen winkeldiefstal. De privacyaspecten hiervan – het is bijvoorbeeld in principe mogelijk om ongemerkt informatie te verzamelen over wat iemand allemaal bij zich heeft – leiden tot veel discussie.²⁰

Tenslotte moet nog de rol worden vermeld die GPS, het bekende Global Positioning System, kan spelen bij toezicht. Behalve voor navigatiedoeleinden kan dit systeem namelijk ook worden gebruikt om de precieze locatie van een persoon (‘persons location’) of een zaak (‘asset location’, bijvoorbeeld van een auto) te bepalen. Wanneer deze informatie vervolgens (bijvoorbeeld via een GSM-verbinding) wordt doorgegeven aan een meldkamer kan dit de opsporing na diefstal sterk vereenvoudigen. Toegepast bij personen (in de vorm van een beveiligde enkelband) maakt dit systeem elektronisch huisarrest op eenvoudige wijze mogelijk.

2.4 Opsporing en vervolging

Veel van de technieken die hierboven zijn beschreven zijn niet alleen geschikt voor toezicht ten behoeve van preventie, maar kunnen ook worden gebruikt bij opsporing en vervolging, dat wil zeggen nadat een strafbaar feit is gepleegd.

Een voor de hand liggend voorbeeld is natuurlijk het gebruik van camerabeelden om een afbeelding van de dader van een delict te verkrijgen. Daarvoor is weinig meer nodig dan dat de beelden enige tijd worden bewaard en dat ze van voldoende kwaliteit zijn om bijvoorbeeld een gelaat te herkennen. Het beeldmateriaal kan dan dienen als

¹⁹ Het eerder aangehaalde rapport van de Commissie Criminaliteit en Technologie bevat een meer uitgebreide beschrijving van deze technieken.

²⁰ Een uitgebreid rapport over RFID met aandacht voor zowel technische als privacyaspecten is gepubliceerd door het Amerikaanse Government Accountability Office (GAO), *Information Security, Radio Frequency Identification Technology in the Federal Government*, WWW, <www.gao.gov/new.items/d05551.pdf>, geraadpleegd 12 oktober 2005.

bewijsmiddel. Technieken voor automatische gelaatsherkenning kunnen in dit verband in principe uitstekende diensten bewijzen, aangezien deze het tijdrovende bekijken van beeldmateriaal door opsporingsambtenaren wellicht voor een groot deel overbodig kunnen maken.

Ook communicatiegegevens (verkeers- zowel als locatiegegevens) kunnen een belangrijke rol spelen bij de opsporing van strafbare feiten, mits deze gegevens voldoende lang bewaard blijven. In het eerder genoemde ontwerp-kaderbesluit 12894/05 van de Raad van Europa d.d. 3 oktober 2005 wordt uitgegaan van een basisbewaartermijn van 12 maanden, hetgeen in de meeste gevallen waarschijnlijk wel voldoende is. De mogelijkheid wordt echter opengehouden dat lidstaten voor bepaalde typen gegevens een kortere termijn hanteren, zo lang die maar niet korter is dan 6 maanden. Deze laatste termijn lijkt in het kader van opsporing aan de krappe kant, het komt regelmatig voor dat een onderzoek naar strafbare feiten aanmerkelijk meer tijd in beslag neemt.

Het gebruik van biometrische gegevens, zoals bijvoorbeeld vingerafdrukken, in de opsporing kent natuurlijk al een lange geschiedenis. Veel van deze technieken zijn zelfs specifiek ontwikkeld met het oog op de opsporing. Met name het gebruik van DNA-profielen heeft de laatste jaren een enorme vlucht genomen. Een belangrijke reden is de betrouwbaarheid die met deze techniek wordt geassocieerd: de kans dat twee personen precies hetzelfde DNA-profiel hebben zou – afhankelijk van het aantal kenmerken in het profiel – in het algemeen kleiner zijn dan één op een miljard.²¹

Net als in het geval van vingerafdrukken is identificatie door middel van DNA alleen mogelijk wanneer zowel DNA-materiaal afkomstig van de plaats-delict als vergelijkingsmateriaal van mogelijke daders beschikbaar is. Sinds 1 februari 2005 is door de inwerkingtreding van de ‘Wet DNA-onderzoek bij veroordeelden’ de mogelijkheid geopend om standaard DNA-materiaal af te nemen bij bepaalde groepen veroordeelden (in eerste instantie gaat het daarbij om veroordeelden van ernstige gewelds- en zedenmisdrijven). Hierdoor kan sneller dan voorheen een DNA vergelijkings‘bank’ worden aangelegd.

Toepassing van dit soort technieken kan gevolgen hebben voor de (straf)rechtspleging. Bewijsmateriaal dat verkregen is met behulp van geavanceerde technologie moet natuurlijk net zo goed als bijvoorbeeld een ‘ouderwetse’ getuigenverklaring worden getoetst op validiteit en betrouwbaarheid. Rechters ondervinden hier in toenemende mate problemen mee en moeten dan vaak blindvaren op getuigenissen van deskundigen. Aangezien het gebruik van technisch bewijs eerder zal toe- dan afnemen is aandacht voor dit probleem van groot belang.

2.5 Slotbeschouwingen met betrekking tot toezichttechnologie

De toekomst van technologie voor toezicht lijkt de combinatie van verschillende technieken. Digitalisering van de informatie, zo blijkt, maakt bovendien gebruik mogelijk op een wijze die tot voor kort ongekend was: niet alleen de (passieve) waarneming en eventueel de registratie daarvan, maar thans kunnen ook voor analyse

²¹ Zie voor achtergrondinformatie over gebruik van DNA profielen bijvoorbeeld B. Budowle, G. Carmody, R. Chakraborty & K.L. Monson, ‘Source attribution of a forensic DNA profile’, in: *Forensic Science Communications*, July 2000, ISSN 1528-8005.

en interpretatie en het aanzetten tot actie apparaten worden ingezet. Het gebruik van videocamera's zoals op Amerikaanse luchthavens, in combinatie met beeldherkenningssoftware en gekoppeld aan achterliggende registraties vormt een voorbeeld. Deze technieken worden ook reeds ingezet als antwoord op *hooliganism* en in de plaats van clubkaarten en kaartjescontrole.

Ook vingerafdrukken en DNA-technologie kunnen tot de toezichttechnologie worden gerekend. Niet alleen waar zij worden ingezet als beheersinstrument, bijvoorbeeld voor het verkrijgen van toegang tot afgesloten ruimtes, maar ook omdat zij reconstructie achteraf mogelijk maken. Ook de opkomst van biometrie is vooral verklaarbaar als een gevolg van de digitalisering.

In algemene zin kan een aantal aspecten worden onderscheiden waarvan het belang en de invloed op maatschappelijke ontwikkelingen aanmerkelijk zijn toegenomen.

1. Technologie

De wereld wordt steeds technischer. De technologische ontwikkelingen hebben zich in de afgelopen 150 jaar in een nauwelijks te volgen tempo aaneengeregen. In dit korte tijdsbestek ondervinden we niet alleen de innovaties van de industriële revolutie, maar wordt het industriële tijdperk zelf al weer opgevolgd door het informatietijdperk. De toepassingen van de technische vindingen zijn talrijk en divers, en vinden plaats overal in de samenleving. Gebruik van technologie voor toezichtdoeleinden is in dit licht bezien dan ook niet bijzonder. Eerder is technologie voor toezichtdoeleinden vanzelfsprekend te noemen, omdat naast het feit dat de technieken nu eenmaal ook goed toepasbaar zijn voor het uitoefenen van toezicht, de samenleving als geheel een veel technischer karakter heeft gekregen, zodat toezicht zich ook eigenlijk niet meer buiten dit technische kader kan afspelen.

2. Management

De technologie doet een verscheidenheid aan mogelijkheden ontstaan, in complexe relaties. Management blijkt dan ook een steeds belangrijker aspect te worden in de uitvoering van taken, aanvankelijk nog vooral in het bedrijfsleven, maar later ook bij overheidsorganisaties. Technologie is een belangrijk hulpmiddel, bijvoorbeeld voor planning, controle en communicatie.

3. Rationaliteit

Het ontstaan van keuzemogelijkheden en de aanwezigheid van alternatieven brengt met zich mee dat mensen steeds rationeler moeten omgaan met beslissingen. Het rationele mensbeeld doet zich dan ook steeds sterker gelden.²² Door de toegenomen welvaart en de daar mee samenhangende economische zelfstandigheid van personen ontstaat een proces van individualisering. Het belang van sociale structuren en van groepsverbanden wordt minder, en soms zelfs staan zij in de weg aan het bereiken van individuele doelstellingen.

Deze aspecten zijn mede verantwoordelijk voor een aantal hierna te noemen tendensen, of versterken deze.

²² Zie bijvoorbeeld M.C. Jensen & W.H. Meckling, 'The Nature of Man', *Journal of Applied Corporate Finance* 1994-2, p. 4-19.

Globalisering

Tengevolge van de technologie is er meer mobiliteit en versnelde globalisering. Dit komt tot uiting in gemakkelijkere fysieke verplaatsingen en in gemakkelijkere uitwisseling van communicatie, bijvoorbeeld door middel van het internet en mobiele telefonie. De globale, maatschappelijke ordening zoals we die kenden is aan het veranderen en dat maakt sturen, beheersen, controleren en het behouden of verkrijgen van overzicht moeilijker, omdat er meer onzekerheden ontstaan.

Bestendigheid tegen weerstanden

Het gebruik van technologie is een alledaags verschijnsel, en in die zin is het dan ook heel gewoon dat technologie ook wordt toegepast voor toezichtdoeleinden en voor juridische doeleinden in brede zin. Wat ook heel gewoon is, is dat de implementatie van nieuwe technologische ontwikkelingen altijd met maatschappelijke weerstand te maken krijgt. De industrialisatie, bijvoorbeeld, zou leiden tot massale werkloosheid, en dus tot grote armoede. De daarop volgende ‘informatie revolutie’ zou leiden tot massale werkloosheid, ditmaal onder kantoorpersoneel. En zowel voor de fabrieksarbeiders als voor de kantoorwerkers zou slechts geestdodende repeterende arbeid resten, gestuurd door het ritme van de automatisering. Wat er daadwerkelijk is gebeurd, is een hogere kwaliteit van de arbeid, mondiaal een hogere arbeidsproductiviteit, een grotere arbeidsparticipatie (voor mannen en voor vrouwen), daling van de kindersterfte en stijging van de levensverwachting, kortom meer welvaart. Ook toezichttechnologie roept overeenkomstige, behoudende reacties op, maar zal de weerstanden evenzeer overwinnen.

Gebruiksgemak voor allen

Technologie kent vele nuttige toepassingen. Niettegenstaande het hiervoor aangehaalde proces van assimilatie, worden de technologische toepassingen steeds laagdrempeliger toegankelijk. Eenvoudiger bediening, compactere afmetingen en lagere prijzen zorgen ervoor dat allerlei apparaten die voorheen in een professionele omgeving werden gesitueerd tegenwoordig ook door consumenten worden gebruikt. Er is echter ook een schaduwzijde. Het is tegenwoordig ook veel gemakkelijker voor individuen, zonder veel technische kennis en zonder organisatorische inbedding, met behulp van moderne technologie terroristische of andere criminele activiteiten te ondernemen, waarvan de potentiële schade een enorme omvang kan aannemen. Computervirussen en de terroristische aanslagen in en met het openbaar vervoer zijn daarvan een goed voorbeeld. Maar het is ook goed denkbaar de energievoorziening of de drinkwatervoorziening te ontregelen. De vragen met betrekking tot de uitdijende werking waartoe het gebruik van toezichttechnologie aanleiding geeft, dienen mede beoordeeld te worden tegen deze achtergrond van toegenomen reikwijdte van terroristische en andere criminele activiteiten, die in sommige gevallen ook nog eens ondernomen worden door nieuwe en onbekende daders.²³

²³ Ook op grond van het zogenoemde ‘voorzorgsbeginsel’ lijkt de uitkomst onontkoombaar dat wanneer het risico groter wordt (hier omdat zowel de kans als de potentiële schade toenemen) eerder tot de toepassing van toezichttechnologie zal worden besloten. Zie over het voorzorgsbeginsel b.v. W.Th. Douma, ‘The precautionary principle’, <http://www.eel.nl/virtue/precprin.htm>. (Icelandic legal journal *Úlfjótur*, 1996, Vol. 49, nrs. 3/4, p. 417-430) en R. Pieterman & J.C. Hanekamp, *The Cautious Society? An Essay on the Rise of the Precautionary Culture*, Zoetermeer: Heidelberg Appeal Nederland 2002.

Normverschuivingen

Wanneer de technologie voorhanden is, dan is te verwachten dat daarvan ook gebruik wordt gemaakt in het kader van toezicht en opsporing en dat daartoe specifieke en eigentijdse toepassingen worden ontworpen. Doorslaggevend daarbij zijn natuurlijk de verwachte effectiviteit en efficiëntie. Inzet van technologie heeft alles te maken met verhoogde doelmatigheid en met kosten. Daarnaast is het zo dat gebruik van technologie ook met normverschuiving te maken heeft, en wel tweeledig. Wat we zien is dat technologie dingen mogelijk maakt die eerst niet mogelijk waren. Of het nu gaat om, bijvoorbeeld, thuishopiëren, interactieve televisie of in vitro fertilisatie, nieuwe mogelijkheden maken bestaande normen minder vanzelfsprekend. Normen blijken tijdsgebonden te zijn.²⁴ In de tweede plaats moeten we onderkennen, dat dat dan natuurlijk ook geldt voor toepassing van technologie voor toezichtdoeleinden, opsporing of handhaving. Dit geldt zowel voor de gebruikers die deze technologie introduceren als degenen die zich hiertegen willen verzetten. Ook overheidssdienaren tonen zich daarbij niet zelden creatief, hun gedrag staat daarmee soms op gespannen voet met de eis van wetmatigheid van bestuur. Het versturen van smsjes aan bij providers opgevraagde mobiele telefoonabonnees is daarvan mogelijk een voorbeeld al kan het tegendeel ook beweerd worden. Het lijkt immers niet wenselijk dat voor alle nieuwe toepassingen van beschikbare technologie steeds persé eerst een wetswijziging nodig is. Dat zou politie en justitie op voorhand in een achterstandspositie manoeuvreren. Wel is het zo, dat creatieve omgang met technologie, of dat nu binnen de bestaande juridische kaders mogelijk is of dat daartoe nieuwe wetsvoorstellen worden gedaan, juridische evaluatie behoeft.

3. Juridische beschouwingen; problemen van afweging

Wat kan als probleem worden ervaren bij het gebruik van toezichttechnologie? Zonder te willen claimen dat hiermee alle problemen zijn geïnventariseerd, zal in het kader van dit artikel aandacht worden besteed aan vijf denkbare vraagpunten. In de eerste plaats is dat het vraagstuk van de veronderstelde inbreuk op het grondwettelijke recht op bescherming van de persoonlijke levenssfeer. In de tweede plaats wordt aandacht besteed aan de vraag of toezichttechnologie door de overheid steeds zou moeten worden beoordeeld in het licht van de strafrechtelijke en in het bijzonder strafvorderlijke regels en in het bijzonder die met betrekking tot de toelaatbaarheid van dwangmiddelen. Toezichttechnologie kan, ten derde, ook een functie hebben met betrekking tot sociale controle en daardoor onverwachte opbrengsten hebben. In de vierde plaats kan toezichttechnologie leiden tot een rechtvaardiger allocatie van middelen, waarmee het beginsel van solidariteit is gediend. In de moderne wereld wordt door vrijwel iedereen kosten-effectiviteit nagestreefd. In juridisch relevante toepassingen, met name wanneer het gaat om het beoordelen van overheidsoptreden en in het bijzonder bij gebruik van toezichttechnologie vertaalt dit streven zich in de beginselen van subsidiariteit en proportionaliteit. Aan deze vijf aspecten worden hierna enige overwegingen gewijd.

²⁴ Zie voor een conceptueel model van de relatie tussen technologie, maatschappelijke ontwikkelingen en recht P. Kleve, *Juridische iconen in het informatietijdperk*, (diss.), Rotterdam/Deventer: Sanders/Kluwer 2004, p. 22 e.v., waarin recht – het (normatieve?) ‘mogen’ – vooral ook als resultante van technologie en rationeel beslissen wordt weergegeven, als resultante van ‘kunnen’ en ‘willen’.

3.1 Privacy versus veiligheid?

Een argument dat veelal als eerste wordt aangevoerd is dat men de gedachte niet prettig vindt bespied te worden, dat men zich niet vrij voelt, dat men in de gaten wordt gehouden en dat iemands gangen achteraf gecontroleerd kunnen worden. Dit is in zoverre vreemd, dat een straat zonder politie om 'de boel' in de gaten te houden door de meeste mensen evenmin op prijs wordt gesteld. Is het dan wellicht een kwestie van balans, wel toezicht, maar ook weer niet te veel? Dit zou echter weer tot de merkwaardige conclusie leiden, dat we moedwillig willen leven met enige onveiligheid, dat het mogelijk zou moeten zijn nog door de mazen van het net te kruipen.²⁵ O.m. Helsloot wijst er op dat uit veel onderzoek blijkt dat burgers bij het beoordelen van veiligheidsrisico's naar veel meer aspecten kijken dan alleen 'de kans op' en 'het effect van' het risico, en noemt als voorbeelden verkeersdeelname en roken.²⁶

Voor wat betreft de relatie tussen privacy en veiligheid in verband met de toepassing van toezichttechnologie lijkt het veelal te gaan om de vraag hoeveel van onze privacy we bereid zouden zijn op te geven ten faveure van de verhoging van onze veiligheid. Het lijkt er aldus op alsof deze grondrechten niet, of althans slechts moeizaam afgewogen, naast elkaar kunnen bestaan.²⁷ Deze vraagstelling behoeft enige nuancering.²⁸ Nemen we als voorbeeld de uitbreiding van het veiligheidsregime op luchthavens met de verplichte terbeschikkingstelling van persoonsgegevens van reizigers. Ondanks de onmiskenbaar persoonlijke inhoud daarvan, laten we ons de controle van onze bagage inmiddels maar al te graag welgevallen. Waarom zou de controle van onze antecedenten vervolgens op weerstand moeten stuiten? Privacy is een moeilijk eenduidig te omschrijven begrip, omdat onder dit begrip verschillende aspecten van ons persoonlijk leven worden geschaard.²⁹ Tegenwoordig is het in de literatuur populair bij privacy te onderscheiden naar verschillende 'dimensies', waaronder een 'ruimtelijke dimensie'.³⁰ De 'ruimtelijke dimensie' uitgedrukt in termen van bewegingsvrijheid: wanneer er géén controle zou plaatsvinden op luchthavens, zouden we ons dan minder of meer belemmerd voelen in onze vrijheid te gaan en staan al naar het ons belijft? En met betrekking tot de uitbreiding van het veiligheidsregime: als onze antecedenten 'goed' zijn, dan zou het denkbaar zijn, dat

²⁵ Er is wel een opvatting die er van uitgaat dat het in een rechtstaat belangrijk is dat er een zeker percentage 'onopgelost' blijft, ter vermindering van de kans op veroordelingen van onschuldigen, maar men kan zich afvragen of een terughoudend gebruik van middelen die meer informatie omtrent de daadwerkelijke toedracht zouden kunnen verschaffen ondersteunend is aan deze doelstelling.

²⁶ I. Helsloot, 'Fysieke veiligheid', in: E.R. Muller (red.), *Veiligheid. Studies over inhoud, organisatie en maatregelen*, Alphen aan den Rijn: Kluwer 2004, p. 367.

²⁷ Schmidt & Zwenne spreken in dit verband van de twee gezichten van de Januskop. A. Schmidt & G.-J. Zwenne, 'Recht en risico. Kanttekeningen bij het voorstel voor een richtlijn over de bewaring van telecommunicatie-verkeersgegevens', *Mediaforum* 2005-9, p. 302.

²⁸ Zie bijvoorbeeld D. Loukidelis, 'Privacy & Security – Are They Irreconcilable Interests?', *5th Annual CACR/Ontario IPC Privacy & Security Workshop*, University of Toronto, 28-29 oktober 2004. Wel maant hij, evenals schrijvers dezes, politici en overheden tot een rationelere omgang met technologie.

²⁹ Zie b.v. A.J. Nieuwenhuis, *Tussen privacy en persoonlijkheidsrecht*, Nijmegen: Ars Aequi Libri 2001 en P.H. Blok, *Het recht op privacy. Een onderzoek naar de betekenis van het begrip 'privacy' in het Nederlandse en Amerikaanse recht* (diss. Tilburg), Den Haag: Boom 2002.

³⁰ In deze 'dimensiebenadering' wordt naast een 'ruimtelijke dimensie' nog onderscheiden in een 'fysieke dimensie', een 'relationele dimensie' en een 'informatie dimensie'.

controle van onze bagage achterwege kan blijven.³¹ Privacy en veiligheid zijn geen communicerende vaten.³² Er is weinig of niets denkbaar dat meer inbreuk op iemands privacy maakt dan de aantasting van diens lijf, of have en goed, en de voortdurende bedreiging daarvan.

Grondrechten hebben van oudsher een bijzondere betekenis in de relatie tussen overheid en burgers. Er zijn rechten en vrijheden geformuleerd die burgers dienen te beschermen tegen willekeurig gebruik van macht door de overheid. In de loop der tijd is het leerstuk van de horizontale werking van grondrechten tot ontwikkeling gekomen. Het recht op eerbiediging van de persoonlijke levenssfeer, bijvoorbeeld, geldt ook jegens burgers onderling. Was het in vroeger tijden de willekeur van de overheid (of de monarch) waartegen bescherming wenselijk was, in de huidige doorontwikkelde democratische rechtstaat lijkt het ‘gevaar’ niet zozeer meer van de door de burgers gecontroleerde overheid te duchten, maar juist van hen die zich daartegen keren. De bedreigingen komen o.m. van hen die angst zaaien. Burgers worden dan soms angstig de metro te nemen of te vliegen, of voor hun mening uit te komen. Heden ten dage lijkt de overheid eerder dienaar van dat grondrecht, dan (potentiële) schender. De vraag is veeleer welk aspect van privacy op een zeker moment in de tijd zwaarder moet wegen, in het licht van de bedreigingen in die tijd. Het is een kwestie van keuze. De inzet van middelen dient men te beoordelen tegen het antwoord op deze vraag.

Daarbij komt, dat ook voor de vraag of er inbreuk wordt gemaakt op de privacy van iemand, het bestaan van een keuzemogelijkheid een van de relevante criteria is. Hoewel het privacybegrip blijkens de literatuur moeilijk eenduidig te definiëren lijkt, geldt dat veel minder voor de vraag wanneer iets als een *inbreuk* op iemands privacy wordt ervaren. Daarvan lijkt minder snel sprake in situaties waarin er een keuze mogelijk is, of die transparant zijn, of die een voordeel opleveren voor betrokkene. Voor de eerbiediging van de persoonlijke levenssfeer, althans het voorkomen dat daar inbreuk op wordt gemaakt, lijken deze criteria belangrijker dan het formuleren van meer of minder concrete gedragingen, omdat bij deze laatste onvoldoende rekening kan worden gehouden met het persoonlijke karakter van privacy.³³

Toezichttechnologie biedt mogelijkheden die we eerder niet hadden en die ertoe kunnen bijdragen dat we ons juist vrijelijker kunnen bewegen en dat we onbezorgder relaties met onbekenden kunnen aangaan. Het gebruik van toezichttechnologie kan bovendien de dienstverlening verhogen. Wel is het zo dat de keuze voor toepassing van toezichttechnologie, respectievelijk voor het onderhevig zijn aan dergelijk toezicht, niet steeds een kwestie van ‘een keuze hebben’ op individueel niveau wordt.

³¹ Dit is slechts bedoeld als voorbeeld, want hoewel om de hier aangehaalde reden ‘denkbaar’, is het achterwege laten van de controle van de bagage niet erg waarschijnlijk, omdat er immers ook andere risico’s spelen, bijvoorbeeld dat iemand anders iets in de bagage heeft gestopt.

³² B.-J. Koops e.a. (*Veiligheid en privacy in 2030: twee toekomstscenario’s*, Universiteit van Tilburg 2005, p. 6) merken weliswaar op dat “privacy en veiligheid lang niet altijd tegenpolen zijn”, maar schetsen merkwaardig genoeg vervolgens twee toekomstscenario’s met als uitgangspunt dat de keuze voor de een gepaard gaat met aantasting van de ander, en menen dan ook nog eens dat deze opzet meer openingen zal bieden voor beleidskeuzes.

³³ Het is dan ook voorspelbaar dat, gegeven de nieuwe mogelijkheden voor de verwerking van (ook) persoonsgegevens tengevolge van het internet, te restrictieve verwerkingseisen uit de Wet bescherming persoonsgegevens plaats zullen maken voor een in beginsel veel vrijer gebruik van persoonsgegevens, onder de condities van transparantie en rechtsbeschermingsmogelijkheden.

In deze zin ontwikkelt het vraagstuk van privacybescherming zich dan ook breder dan de tot nog toe gebruikelijke benadering, waarin de keuzemogelijkheid van het individu meer centraal staat. In relatie tot de toepassing van toezichttechnologie krijgt bescherming van privacy naast het individueel niveau ook een meer collectief karakter, en blijkt ‘bescherming’ van het grondrecht ook te liggen in het toelaten van selectieve ‘inbreuken’ daarop. Dit lijkt paradoxaal, maar is goed verklaarbaar vanuit het relatieve nut van de toepassing. Waar het een individueel niveau betreft, zal de wetgever voorzichtiger moeten zijn met het veralgemeniseren van dit niveau, om te voorkomen dat op voorhand het nuttig ervaren gebruik van technologie beperkt of onmogelijk gemaakt wordt.³⁴ De bredere context van de beschermingsomvang zal in Nederland tot een bijstelling van de taakopvatting van het College Bescherming Persoonsgegevens moeten leiden. Uit onderzoek naar opvattingen over de afweging tussen privacy en veiligheid, zoals ten aanzien van DNA-registratie en het gebruik van omvangrijke privacy-gevoelige databanken blijkt bij bevolkingsenquetes veelal dat een groter belang wordt gehecht aan het veiligheidsaspect dan aan overwegingen van privacy.³⁵

3.2 Het principe van de verdachte

Naast, of in het verlengde van het argument dat toezichttechnologie inbreuk maakt op de privacy, wordt wel aangevoerd dat een ongedifferentieerd gebruik inbreuk maakt op het rechtsbeginsel dat de toepassing van dwangmiddelen beperkt tot ‘verdachten’, dan wel dat daardoor eenieder wordt aangemerkt als verdachte. Dat deze argumenten in elkaars verlengde liggen blijkt hieruit, dat gebruik van toezichttechnologie tegen verdachten kennelijk niet als omstreden wordt ervaren. Dat ligt ook voor de hand, aangezien de inzet van dwangmiddelen nu juist bedoeld is om inbreuk op iemands persoonlijke levenssfeer te (mogen) maken. Kennelijk gaat het er dus om dat ook niet-verdachten zich de toepassing van toezichttechnologie moeten laten welgevalen en waar toezichttechnologie als dwangmiddel wordt gekwalificeerd maakt die toepassing inbreuk op de persoonlijke levenssfeer. In deze zienswijze is het dan zo dat, ten eerste, men de status van ‘verdachte’ zou dienen te hebben vooraleer men aan overheidscontrole mag worden blootgesteld en, ten tweede, dat toezichttechnologie (steeds) als dwangmiddel gekwalificeerd zou moeten worden.

Om te beginnen is het niet zo, dat overheidsfunctionarissen, waaronder politie en justitie, steeds alleen mogen wat nauwkeurig is omschreven. Zij mogen tot op zekere hoogte, net als gewone burgers, mensen vragen stellen, mensen opbellen, dus ook mensen sms-berichten sturen. Deze activiteiten steunen niet op enig dwangmiddel – het staat burgers dan ook vrij niet te antwoorden – noch zijn zij voorbehouden voor ‘verdachten’.³⁶ Dat mensen het wellicht niet prettig vinden door de politie te worden aangesproken, dat ze wellicht toch geïntimideerd raken, brengt wel met zich mee dat de politie er op een verstandige manier mee om moet gaan, maar dat is op zichzelf onvoldoende grond – en het zou ook niet wenselijk zijn – om het stellen van vragen met beperkingen te omgeven. Zelfs niet in die gevallen waarin men door te weigeren

³⁴ Zie bijvoorbeeld de strikte uitlegging van richtlijn 95/46/EG op het vermelden van persoonsgegevens op een webpagina, HvJ 6 november 2003, *Lindqvist*, C-101/01, <http://curia.eu.int/>.

³⁵ H. Elffers, *Onderzoek in het kader van de Onderzoeksschool Maatschappelijk Veiligheid*, 2000.

³⁶ Zie ook de bijdrage van L.J.J. Rogier in deze bundel over Toezicht op de naleving in de Algemene wet bestuursrecht. Vgl. voorts het vragen door de politie aan een bevolkingsgroep mee te werken aan een (vrijwillig) DNA-onderzoek.

te antwoorden alsnog de status van verdachte zou verkrijgen, waardoor er vervolgens dwangmiddelen mogen worden toegepast.³⁷

Het leggen van een verband tussen de ontvangst van een sms van de politie en de status van verdachte is dan ook vergezocht. De politie wil in het kader van het onderzoek in contact treden met personen, ‘getuigen’, die zich ten tijde van de voetbalrellen in de buurt van het stadion bevonden, teneinde deze personen te vragen of zij iets hebben gezien dat van belang kan zijn voor dat onderzoek. Daartoe kan zij in de buurt gaan rondvragen en, bijvoorbeeld, gaan aanbellen bij bewoners, of bij de eerstvolgende thuiswedstrijd van Feyenoord alle bezoekers vragen stellen. De keuze voor het sturen van een sms lijkt in zoverre aantrekkelijker, dat (bijna) uitsluitend mensen die inderdaad op de betreffende tijd in de buurt van het stadion waren worden ‘lastig gevallen’, dat dit kan in een fractie van de menscapaciteit die anders nodig zou zijn en tegen veel lagere kosten en dat een smsje van de politie ook voor betrokkenen minder tijdrovend is en (wellicht) minder intimiderend overkomt, zo dit zou spelen.³⁸

Meer in het algemeen is het ook niet zo dat iemand verdacht moest zijn van het begaan van een concreet feit om aan overheidscontrole onderhevig te worden gemaakt.³⁹ In veel gevallen is de bevoegdheid tot het uitoefenen van controle in de wet omschreven. Duidelijke voorbeelden zijn wel de verplichte aangifte voor de inkomstenbelasting,⁴⁰ maar ook de flitspalen. Controle op de naleving van de maximumsnelheid maakt niet dat alle weggebruikers ‘verdachten’ worden. En de eventuele geautomatiseerde controle van de aangifte inkomstenbelasting, bijvoorbeeld door deze te koppelen aan gegevens uit andere bronnen, is geen principiële uitbreiding van de belastingcontrole. De terbeschikkingstelling van de gegevens – de ‘koppeling’ van bestanden – dient op zichzelf reeds gebaseerd te zijn op een wettelijk voorschrift. Wel is het zo, dat omdat we tegenwoordig gegevens met behulp van computers eenvoudiger kunnen vergelijken (controleren), dit met het oog op die mogelijkheden eerder, of zelfs speciaal, tot zulke wettelijke voorschriften aanleiding zal kunnen geven.

3.3 Technologie en sociale controle

Het gebruik van toezichttechnologie, zo bleek hierboven reeds in het voorbeeld van de belastingcontrole, is niet altijd een uitbreiding van of op bestaande bevoegdheden. Het is veelal een middel waarmee bestaande bevoegdheden aan effectiviteit of aan efficiency winnen. Daarbij zij vermeld, dat het simpele feit dat iets nuttig is, of nuttiger dan voorheen, als vanzelf ook tot een zekere normverschuiving leidt. Belangrijk is echter dat men een open oog houdt voor het feit dat technologie

³⁷ Naast de opvatting dat ongedifferentieerd overheidstoezicht de kring van verdachten (ontoelaatbaar) zou uitbreiden, kan de opvatting geplaast worden, dat dergelijk toezicht juist zal leiden tot inperking van de kring van verdachten.

³⁸ Wat wel nodig is, is een onderzoek naar de resultaten van deze actie. Een verminderde ‘belasting’ voor burgers is niet voldoende om de keuze te legitimeren, de belasting moet ook gerelateerd worden aan het bereikte resultaat. Voorts is een dergelijk onderzoek nuttig, omdat eventuele andere effecten kunnen blijken, bijvoorbeeld dat men genegen zou kunnen zijn langs deze wijze eerder informatie te verstrekken omdat voor andere personen (de relschoppers) verborgen blijft dat er contact met de politie is geweest, of, integendeel, dat men vanwege de vermindering van anonimiteit juist weigerachtig is.

³⁹ Zie art. 5:20 lid 1 Algemene wet bestuursrecht op grond waarvan “een ieder” verplicht is aan een toezichthouder in de zin van deze wet alle medewerking te verlenen.

⁴⁰ Waarbij het overigens voorspelbaar is dat bij afwezigheid van controle het aantal *free riders* – niet-juridische term voor ‘fraudeurs’ – bijna de volledige populatie zal beslaan.

doorgaans vooral ‘middel’ is, ter realisering van allerlei aspecten die mensen nuttig vinden. Toezichttechnologie is in deze zin dienstig aan ‘normhandhaving’, net zoals recht ook dienstig is aan normhandhaving.

Wanneer mensen op vakantie gaan, dan vragen ze de burens de boel een beetje in de gaten te houden. En dat de politiewagen wat vaker langsrijdt is dan ook niet onwelkom. Wanneer er iemand zich bij het verlaten huis van de vakantiegangers ophoudt, dan wordt de vraag van de burens, of zij ‘wellicht kunnen helpen’ ook op prijs gesteld. En vroeger sprak men elkaar nog wel eens aan op gedrag. Dat gebeurt tegenwoordig minder. Daarvoor zijn verschillende redenen aan te voeren. In algemene zin kan verwezen worden naar de hierboven aangehaalde tendensen van toegenomen mobiliteit en van individualisering. Meer concreet ziet men ook dat dergelijke interventies niet zonder risico’s zijn.

De sociale controle en sociale cohesie, die enkele decennia geleden nog redelijk voor zich spraken, bestaan niet meer, althans kunnen niet meer bestaan in de oude vorm. Dat sociale controle een nuttige functie heeft en dat sociale cohesie als het ware het bindmiddel van een samenleving vormt, daarover lijkt men moeilijk van mening te kunnen verschillen. Door middel van technologie kan de leemte van de afkalvende sociale controle worden opgevuld. Door middel van technologie kunnen sociale controle en sociale cohesie opnieuw vorm worden gegeven. Wanneer in concrete gevallen moet worden beoordeeld of toezichttechnologie rechtmatig wordt toegepast, is het wenselijk behalve voor de kosten en de nadelen ook oog te hebben voor de opbrengsten en de maatschappelijke voordelen.

3.4 Technologie en solidariteit

De keuze voor toepassing van toezichttechnologie lijkt vooral een kwestie van doelmatigheid. Hoewel *efficiency* als norm mogelijk voor meer gangbaar wordt gehouden voor het private domein, spelen in het publieke domein nauwelijks andere afwegingen dan in het private domein. En alhoewel het daarom soms lijkt alsof de acceptatie van doelmatigheidsoverwegingen in het private domein wat groter is dan in het publieke domein, is het dan ook niet vreemd te zien dat verhoogde doelmatigheid in het private domein evenzeer aan kritiek bloot staat, veelal onder de noemers van commercieel gewin en verminderde service. Wanneer men deze kritiek nader analyseert, blijkt het veelal te gaan om het in rekening brengen van activiteiten die voorheen niet of te weinig werden betaald, respectievelijk stoppen met activiteiten die voorheen niet of te weinig werden betaald.⁴¹ Wat het publieke en het private domein daarin gemeen hebben, is dat betrokkenen zullen instemmen met de voordelige effecten voor henzelf tengevolge van het belasten van anderen, maar niet willen bijbetalen tengevolge van hun eigen deficit. In beide situaties leidt dit tot een conservatieve grondhouding. Doelmatigheid als criterium is evenwel van groot belang als waarborg voor solidariteit.⁴² De inzet van technologie kan de doelmatigheid bevorderen.

⁴¹ In deze termen kan ook worden gesproken over, bijvoorbeeld, het afstoten van niet-renderende activiteiten (w.o. het opheffen van niet-renderende openbaar-vervoertreinen) of het niet overgaan tot het exploiteren van verliesgevendende activiteiten (w.o. het weigeren hogere risico’s te verzekeren zonder hogere premiebetaling).

⁴² En in een commerciële omgeving als waarborg voor klantenbinding.

Belangrijk is immers de vraag te stellen hoe lang burgers bereid zijn financieel bij te blijven dragen aan een herverdelingsorganisatie die (relatief) duur is, en waarbij niet steeds die burgers worden bereikt waarvoor de herverdeling is bedoeld en soms wel burgers waarvoor de herverdeling niet is bedoeld. Van belang hierbij zijn de hierboven aangevoerde algemene tendensen van toegenomen maatschappelijke complexiteit, van toegenomen mobiliteit en van individualisering. Veel herverdelingsorganisaties zijn gegrond op het beginsel van solidariteit. Of dat nu gaat om werkloosheidsuitkeringen, (sociale) verzekeringen, huurtoeslag of bijstand, of om contributies aan fondsen van kerken, maatschappelijke organisaties tot nut van het algemeen of 'goede doelen' bijvoorbeeld. Als gevolg van de hier bedoelde tendensen is het veel moeilijker geworden de mensen te bereiken die gerechtigd zijn tot de herverdelingsgelden, 'solidariteitsfondsen', en misbruik of frauduleus gebruik van dergelijke fondsen te voorkomen. Wanneer daardoor bij contribuanten de indruk gaat ontstaan dat het geld toch niet goed terecht komt, zal de bereidheid aan dergelijke fondsen bij te dragen alleen maar afnemen. De solidariteit komt onder druk en brokkelt af. Het gebruik van technologie die het uitvoeren van toezicht en controle efficiënter maakt, waardoor b.v. frauduleus gebruik van voorzieningen kan worden verminderd, mag in zekere zin zelfs worden vereist.

In feite is de uitvoering van complexe wetgevingstrajecten niet eens meer mogelijk zonder gebruik te maken van technologie. Of nog duidelijker, vaak krijgt het ontwerp van complexe wettelijke regelingen mede vorm door de wijze waarop de regeling op geautomatiseerde wijze kan worden uitgevoerd.⁴³ Het creëren en behouden van draagvlak hangt sterk samen met een juiste naleving, zeker op langere termijn. Het gebruik van technologie als beheerinstrument en als middel ter ondersteuning van en controle op correcte naleving, zou contribuanten daarover grotere zekerheid kunnen verschaffen. Doordat we computers hebben kunnen we grove regelingen verfijnen, zodat beter rekening kan worden gehouden met relevante individuele omstandigheden. Juist in de mogelijkheid te differentiëren kan men recht doen aan het gelijkheidsbeginsel.⁴⁴ Waar er minder informeel toezicht mogelijk is tengevolge van een grotere afstand tussen contribuant en ontvanger, zou inzet van technologie kunnen bijdragen aan het waarborgen van solidariteit.

3.5 Subsidiariteit en proportionaliteit

Het gebruik van toezichttechnologie kan niet in het algemeen als niet verenigbaar met het grondrecht op bescherming van de persoonlijke levenssfeer worden geoordeeld. Dat komt o.m. omdat veiligheidsdoeleinden niet haaks staan op de persoonlijke levenssfeer, maar als een aspect daarvan kunnen worden aangemerkt. Voorts kan men stellen, dat het recht op eerbiediging van de persoonlijke levenssfeer niet zo absoluut is, dat andere belangen niet mogen worden afgewogen. En in de derde plaats is betoogd dat de reikwijdte van het privacybegrip, zowel als de invulling daarvan, mede begrepen moeten worden tegen de achtergrond van de technologische ontwikkelingen en van de maatschappelijke ontwikkelingen.

Eveneens is beargumenteerd dat ongedifferentieerde toepassing niet in strijd hoeft te zijn met het beginsel van de verdachte. Dat komt, omdat toezichttechnologie niet zelf

⁴³ Men denke maar aan de studiefinanciering en de OV-jaarkaart voor studenten.

⁴⁴ Zie ook P. Kleve, *Rechtsvragen over informatietechnologie. Ontwikkeling, stand van zaken en betekenis van het informaticarecht*, Lelystad: Vermande 1996, p. 190.

als ‘dwangmiddel’ kan worden aangemerkt. Toezichttechnologie is een middel, dat zowel binnen als buiten de sfeer van strafvorderlijke bevoegdheden kan worden gebruikt. Het zich schikken naar toezicht, en verplichtingen mee te werken aan controles, is mogelijk zonder dat daarvoor de status van ‘verdachte’ moet worden toegekend.⁴⁵

Vanuit een andere invalshoek is gewezen op enkele positieve effecten, zoals de mogelijkheden door middel van technologie de burgerservice te verhogen en de nuttige bijdrage aan de respectering en naleving van grondrechten.

Tenslotte, zo is gebleken, is evenmin vereist dat gebruik van toezichttechnologie eerst mogelijk zou zijn na daartoe strekkende wetwijzigingen. Technologie kan goed worden toegepast binnen bestaande wettelijke kaders. Daarbij is wel naar voren gebracht, dat het gebruik van technologie – het gebruik in de samenleving in het algemeen en de bijzondere mogelijkheden voor toezicht – tot veranderende normen kunnen leiden.

Bij de toepassing van toezichttechnologie dient men, zoals ook bij andere middelen, zich voldoende rekenschap te geven van de juridische vragen die er van geval tot geval kunnen spelen. Het zijn met name de beginselen van proportionaliteit en van subsidiariteit die de reikwijdte van de betreffende toepassing (juridisch) zullen afbakenen.⁴⁶ In het voorbeeld van de smsjes van de Rotterdamse politie kan goed worden verdedigd dat de toepassing binnen deze afwegingskaders zijn gebleven, zonder dat de potentiële dreiging wordt gebagatelliseerd. Een ander voorbeeld is de proef met cameratoezicht medio 2005 in het centrum van Groningen.⁴⁷ De camera’s draaiden niet continu, maar werden geactiveerd op basis van door aan de camera’s gekoppelde microfoons waargenomen geluid. Hoewel men kan zeggen dat het toezicht continu was, werd het systeem alleen geactiveerd indien daar op basis van het geregistreerde geluid aanleiding toe was. Het is ook hierom een goed voorbeeld, omdat de proportionele toepassing volgend uit de *beperking* van ‘inbreuk’ op de privacy juist vanwege de moderne technologie kon worden gerealiseerd.

Bij de regeling van de juridische randvoorwaarden, evenwel, dient men zich te realiseren dat een al te terughoudend gebruik vooral in het voordeel van criminelen kan uitpakken. In relatie tot het beginsel van de verdachte moet daarbij gewicht worden toegekend aan de situatie dat de dreiging anoniemer en onbestemder is geworden. Wat ook in de afwegingen een rol kan spelen, is dat met toezichttechnologie niet alleen repressie kan worden nagestreefd, maar ook preventie, naast serviceverhoging en kostenbesparing (voor ‘consument’ en ‘belastingbetaler’). Voor wat betreft de eisen die men kan stellen aan het gebruik van toezichttechnologie, dient men zich te realiseren dat technologie en organisatie zodanig mogelijk zijn, dat niet steeds alle informatie op de verschillende geleidingen beschikbaar hoeft te zijn. Voldoende is soms dat het beschikbaar is te maken. In het voorbeeld van de Rotterdamse politie schijnen geen namen of adresgegevens ter beschikking te zijn gesteld, maar kon de actie gezien het doel beperkt blijven tot de telefoonnummers. Er

⁴⁵ Zie noot 39.

⁴⁶ Zie de artikelen 5:13 en 5:20 Algemene wet bestuursrecht waarin is bepaald dat een toezichthouder slechts van zijn bevoegdheden gebruik maakt en in het bijzonder slechts inlichtingen vordert voor zover dat redelijkerwijs voor de vervulling van zijn taak nodig is.

⁴⁷ Het College Bescherming Persoonsgegevens had geen bezwaar tegen deze toepassing.

gebeurt veel op het gebied van de zogenoemde *privacy enhancing technology* (PET) en anonimiserings toepassingen.⁴⁸ Vanzelfsprekend moet men nadenken over beveiliging, verlies van data en de eventuele aanspraken die belanghebbenden mogen hebben in het geval van verlies, misbruik of schadeveroorzakend gebruik. In het algemeen lijkt het aan te bevelen de juridische randvoorwaarden steeds kenbaar te maken bij de introductie van het gebruik van technologie.

4. Conclusies

Voor een deel lijkt het erop dat de bezwaren die tegen toezichttechnologie worden aangevoerd erop neerkomen dat we wel de ander aan controle willen onderwerpen, maar niet onszelf. Wij zouden onszelf dan zien als eerbare burgers voor wie controle alleen maar een onnodige beperking van onze privacy oplevert, ja soms zelfs ronduit als beledigend kan worden ervaren, alsof men ervan verdacht wordt een crimineel te zijn. Toch is dat vreemd, want we blijken baat te hebben bij een toezieende overheid.⁴⁹ Wat niet vreemd is, is dat de kritiek wordt verwoord door juristen en door instituties (zoals het College Bescherming Persoonsgegevens, Amnesty International, 'oud links', juridische faculteiten e.d.). Op grond van het rationele mensbeeld is immers goed verklaarbaar waarom van die kant bezwaren worden geopperd.

Voorts lijkt het erop dat de weerstand vooral is terug te voeren tot het assimilatieproces van nieuwe technologie. Het is weerstand tegen de technologie en tegen verandering. Daarbij is het denkbaar dat het niet weten of er een situatie is waarin men aan toezicht blootstaat, hoe ver dat toezicht reikt, wie het uitvoert en wat er verder mee gebeurt mensen een onbehaaglijk gevoel kan bezorgen. Het heeft iets van niet zelf zien maar wel gezien worden. Zonder transparantie rond deze vragen is invoelbaar dat een gevoel van kwetsbaarheid groeit in plaats van afneemt. En dat remt het assimilatieproces, terwijl dat juist zo belangrijk is met het oog op het onderkennen van het nut van de betreffende techniek.

Een conclusie die in de juridische literatuur wat ongewoon is, is dat technologie – ook toezichttechnologie – het juist gemakkelijker mogelijk maakt grondrechten te eerbiedigen en te beschermen.

Een goed voorbeeld van hoe de overheid kan inspelen op nieuwe technologie is de bevraging van omstanders op basis van hun mobiele locatiegegevens. Andere voorbeelden van hoe de overheid goed kan omgaan met nieuwe – en deels onbekende – dreigingen zijn de virtuele slotgracht en het wat langer bewaren van de verkeersgegevens van netwerken. Dat zijn namelijk allemaal voorbeelden van gebruik maken van nieuwe mogelijkheden ten behoeve van een effectievere handhaving van bestaande normen. Dat de norm voor handhaving daarbij wat opschuift is een logisch gevolg van de technologische ontwikkelingen, die overigens in algemene zin brede toepassing kennen waarin het gebruik door bijvoorbeeld politie en justitie geen bijzondere plaats inneemt. Een belangrijk criterium is of het werkt, de effectiviteit moet worden beproefd.

⁴⁸ R. Koorn e.a., *Privacy Enhancing Technologies, Witboek voor beslissers*, 's-Gravenhage: Ministerie van Binnenlandse Zaken en Koninkrijksrelaties 2004.

(http://www.cbppweb.nl/downloads_technologie/Witboek_PET.pdf).

⁴⁹ Zie ook H.O. Kerkmeester, *Recht en Speltheorie* (diss.), Lelystad: Vermande 1989.

In het bovenstaande zijn, na het overzicht van nieuwe technische mogelijkheden bij toezicht, vijf punten van afweging naar voren gebracht. Het betrof 'privacy en veiligheid', het belang van aanwezigheid van een 'verdachte', 'technologie en sociale controle', 'technologie en solidariteit' en kost-effectiviteit. De conclusie moet zijn dat toezichtstechnologie noopt tot een hernieuwde afweging van waarden en belangen. Het recht op privacy – en in het voetspoor van de technologische en maatschappelijke ontwikkelingen ook enkele andere rechten zoals het auteursrecht – zijn aan een herziening toe. De automatische reacties van ijveraars voor dit recht (deze rechten) zijn niet meer adequaat. Het recht op privacy staat niet alleen onder druk in de afweging met het recht op c.q. de wens naar veiligheid, maar ook in de confrontatie met andere rechten, zoals sommige collectieve sociale grondrechten en wenselijkheden, zelfs in confrontatie met het recht op privacy zelf. Immers, de privacy van de ene persoon is de inbreuk op de privacy van de ander. Er schijnt nog steeds een niet onaanzienlijke markt, mogelijk zelfs groeiende markt te zijn voor de produkten van de roddelpers. Mensen willen thuis graag privacygevoelige verhalen lezen over anderen. Belangrijker dan de afweging privacy – veiligheid is misschien nog wel die tussen privacy en recht op informatie. In het eerder aangehaalde Lindqvist-arrest is beslist, dat het publiceren over de gebroken teen van de buurvrouw op het internet een strafbare inbreuk op het recht van privacy kan opleveren. Als dat de trend wordt, kunnen nieuwe interessante publicatiemediën zoals weblogs al weer onmogelijk gemaakt worden voordat ze echt populair zijn. Ook in het licht van claims van sommigen op het recht op anonimiteit, gender-wisseling, leeftijd wisseling – dus claims die verder gaan dan een claim op het recht 'ongestoord zichzelf te zijn' – is een heroriëntering op de gewenste invulling van het recht op privacy uiterst gewenst.

Het inleveren c.q. opnieuw afwegen van grondrechten brengt echter steeds ook de wenselijkheid van een effectieve controle van het gebruik van overheidsmacht met zich mee. Tegenstanders van toezichtstechnologie wijzen behalve op strijd met (grond)rechten en het kostenaspect (of de onbekendheid daarmee) vooral ook op het gevaar van misbruik door overheidsdienaren.

Dit is wellicht het belangrijkste punt van discussie over juridische en maatschappelijke vernieuwing als gevolg van de technologische vooruitgang. Technologie leidt niet alleen op een praktische manier tot toezichtsmogelijkheden, maar op een meer complexe manier tot een nieuwe organisatie van de staatsmacht. De Mulder⁵⁰ betoogt dat een nieuwe vierde macht onvermijdelijk is, vergelijkbaar met de onvermijdelijkheid van het opkomen van een uitvoerende macht nadat het recht niet alleen geschreven, maar ook gedrukt kon worden. Die ontwikkeling leidde tot de grootschalige overheidsbureaucratieën die wij thans kennen. De technische mogelijkheden van computers en internet zullen niet minder ingrijpende gevolgen hebben. Het verschijnen van een nieuwe macht, de toeziende macht, lijkt waarschijnlijk. Mogelijk zien wij dit nieuwe element al verschijnen in de vorm van instituties als Algemene Rekenkamer, Ombudsman, NMA, OPTA en CBP.

De vestiging van de nieuwe macht als gevolg van de nieuwe maatschappelijke omstandigheden zal ingrijpende consequenties hebben voor het recht, voor het functioneren van de rechtsstaat en voor de juridische professie. De groei van de

⁵⁰ Mulder, R.V. De, 'The Digital Revolution: From Trias to Tetras Politica', in: Snellen, I.Th.M. , Donk, W.B.H.J. van de (Eds.), in: *Public Administration in an Information Age. A Handbook*, p 47-56, Amsterdam: IOS Press 1998, ISBN: 90 5199 395 1.

uitvoerende macht leidde tot grootschalige bureaucratieën. Deze hebben hun nut, maar blijken ook tot excessen te leiden. Vooral nog lijkt een systematische aandacht van toezichhouders op het gebruik van toezichttechnologie in democratische rechtsstaten een *conditio sine qua non* voor het voortbestaan daarvan in een globaliserende en steeds technocratischer wordende wereld.