Technische bewijsvergaring

Koops, E.J.

Published in:
Elsa Leiden Magazine

Publication date:
2005

Koops, B.J. (2005). Technische bewijsvergaring: wie wint de machtsstrijd? *Elsa Leiden Magazine, 1*(5), 15-19.

Technische bewijsvergaring: wie wint de machtsstrijd?

Dr. Bert-Jaap Koops is universitair hoofddocent strafrecht & techniek bij TILT, Centrum voor Recht, Bestuur en Samenleving, van de Universiteit van Tilburg.

1. Inleiding

De laatste maanden buitelen de voorstellen voor ruimere bevoegdheden om terrorisme te bestrijden over elkaar heen. Terroristen en de overheid lijken een oorlog te voeren om uit te vechten wie de sterkste is. Maar vrijwel ongemerkt voltrekt zich ook een andere machtsstrijd, een die minstens zo belangrijk is: misdadigers en de overheid strijden om de nieuwste technische snufjes om elkaar te slim af te zijn. Nieuwe mogelijkheden om techniek te misbruiken bij het plegen van misdrijven leiden steevast tot voorstellen voor nieuwe of ruimere bevoegdheden om misdrijven op te sporen.

Wordt de overheid niet té machtig door deze almaar uitbreidende opsporingsbevoegdheden? In dit artikel geef ik een overzicht van een selectie van bevoegdheden die recentelijk zijn ingevoerd of zijn voorgesteld, of die in de nabije toekomst te verwachten zijn, met als doel de machtsstrijd om techniek bij het strafrechtelijk bewijsrecht te belichten.[1]

2. Gegevensvergaring[2]

In februari 2004 werd een wetsvoorstel 'vorderen gegevens' ingediend, dat justitie bevoegdheden geeft om allerlei gegevens bij instellingen en burgers op te vragen – elektronische en papieren.[3] De nieuwe bevoegdheden moeten worden bezien tegen de achtergrond van de informatiemaatschappij, waarin gegevens steeds belangrijker worden. Voor de opsporing lonkt een mekka van bestanden, registraties en computersystemen, waarin over elke verdachte, elk slachtoffer, hun hele familie-, vrienden- en kennissenkring, ja zelfs over hun losse contacten met vreemden en bedrijven, en ook over hun auto's, mobieltjes en bankrekeningen, wel iets te vinden valt. De huidige bevoegdheden om al dergelijke gegevens op te vragen, schieten te kort, en medewerking op vrijwillige basis zorgt voor problemen.[4]

Het nieuwe arsenaal breidt de bevoegdheden voor justitie aanzienlijk uit ten opzichte van de huidige – beperkte – bevoegdheid, art. 125i Sv, die wordt ingeruild voor drie nieuwe hoofdbevoegdheden, voor identificerende, algemene en gevoelige gegevens. Allereerst kan de opsporingsambtenaar op grond van de artikelen 126nc Sv identificerende gegevens opvragen, en wel bij verdenking van een misdrijf. Het gaat hier om naam, adres, woonplaats, geboortedatum en geslacht, en administratieve kenmerken, zoals het nummer van de airmiles-pas, het lidnummer van de sportvereniging, en bankrekeningnummers. De vordering wordt gericht tot personen die dergelijke gegevens verwerken, anders dan voor persoonlijk gebruik. In de praktijk kan de politie hiermee eenvoudig nagaan bij een postorderbedrijf, een videotheek, een supermarkt of een sportvereniging of iemand daar een klant of lid is.

---

[1] Deze selectie is gebaseerd op het onderzoek dat ik het afgelopen jaar, deels in samenwerking met mr. Merel Prinsen en mr. Lonneke Stevens (beide UvT), heb verricht naar diverse bevoegdheden tot het vergaren van technisch bewijsmateriaal. In dit artikel put ik mede uit deze eerdere onderzoeksresultaten.

[2] Zie uitgebreider L. Stevens, B.J. Koops & P. Wiemans (2004), 'Een strafvorderlijke gegevensvergaring nieuwe stijl', *Nederlands Juristenblad* 79 (32), p. 1680-1686.

[3] *Kamerstukken II* 2003/04, 29 441, nr. 2. Zie voorts ook m.b.t. de financiële sector Stb. 2004, 109, en m.b.t. telecommunicatie Stb. 2004, 105. Al deze stukken, alsmede reacties hierop, zijn te vinden op <http://www.gegeven.nl>.

[4] *Kamerstukken II* 2003/04, 29 441, nr. 3, p. 1-2, 17.

De politieagent kan zo verbanden leggen tussen personen, bijvoorbeeld om te kijken wie zoal contact kan hebben met een verdachte fraudeur binnen de golfclub.
In de tweede plaats krijgt de officier van justitie de bevoegdheid om 'andere dan identificerende' gegevens op te vragen (artikel 126nd Sv). Dan gaat het om informatie over een dienst die geleverd is, bijvoorbeeld het soort videobanden dat geleend is, welke boeken iemand hoe lang heeft geleend bij de bibliotheek, of hoeveel boodschappen iemand de afgelopen maand heeft afgerekend met zijn klantenpas, en ook – als de supermarkt dat bijhoudt – welke boodschappen dat precies waren.[5] Het kan dus om zeer privacygevoelige gegevens gaan, en daarom mag de bevoegdheid alleen worden ingezet bij zwaardere misdrijven, namelijk die worden genoemd in artikel 67, eerste lid Sv. Het hoeft echter niet om verdachten te gaan: de officier mag over iedereen gegevens opvragen als hij denkt dat dit nuttig is voor een opsporingsonderzoek. De vordering van deze gegevens kan zelfs betrekking hebben op toekomstige gegevens (art. 126ne). Het gaat dan bijvoorbeeld om video's die iemand in de komende vier weken huurt of boodschappen die hij de komende weken zal doen. De officier kan zelfs, met machtiging van de rechter-commissaris, bevelen dat het bedrijf deze gegevens steeds direct doorstuurt aan justitie.
Met machtiging van de rechter-commissaris kunnen ten derde ook gevoelige gegevens worden opgevraagd, bij zware misdrijven die een ernstige inbreuk op de rechtsorde maken (artikel 126nf). Gevoelige gegevens zijn gegevens over iemands godsdienst, ras, politieke gezindheid, gezondheid, seksuele leven of vakbondslidmaatschap. Boeken of video's over ziektes, seks of godsdienst en boodschappen van suikervrije producten zijn dus gevoelige gegevens. Daarom zou de officier niet zomaar bij elke videotheek, bibliotheek of supermarkt alle gegevens mogen opvragen. Het probleem is alleen dat de gevoeligheid van gegevens niet vooraf kenbaar zal zijn. Daarom kan de officier vermoedelijk gewoon alle gegevens opvragen, en eventuele gevoelige video's of boodschappen als 'bijvangst' tellen.
Naast deze hoofdbevoegdheden worden nog enkele nevenbevoegdheden ingevoerd, zoals ontsleuteling, bevriezing en bewerking van gegevens.
In het licht van de vraagstelling van dit artikel kan over dit wetsvoorstel eenvoudig worden geconcludeerd dat het de overheid machtiger maakt dan voorheen. Justitie zal in de toekomst in principe bij iedereen alle soorten vastgelegde gegevens kunnen opvragen. De bevoegdheden worden weliswaar omkleed met enkele waarborgen, maar kunnen niettemin voor alle gegevens worden uitgeoefend, inclusief de privacygevoeligste gegevens die individuele onverdachte burgers voor zichzelf vastleggen. En ook over onverdachte burgers mogen gegevens worden opgevraagd. Het adagium 'wie niets te verbergen heeft, heeft niets te vrezen', dat veel mensen tegenwoordig lijken te hanteren, is te kortzichtig, omdat burgers door verzoeken van politie bij derden in een kwaad daglicht kunnen komen te staan. Een vraag aan een videotheekhouder of meneer Jansen de afgelopen maand 'Lolita' of andere films met kleine meisjes heeft geleend, zal de baliemedewerker de volgende keer toch met andere ogen doen kijken als Jansen de videotheek binnenloopt.

3. Bewaarplicht verkeersgegevens[6]

Verkeersgegevens zijn gegevens over telecommunicatieverkeer: wie heeft met wie gebeld, wanneer en hoe lang, en waarvandaan? Welke netpostberichten heeft iemand verstuurd naar wie, en welke weblocaties zijn bezocht? Sinds het begin van deze eeuw wordt gesproken over een mogelijke bewaarplicht voor dergelijke verkeersgegevens, met name in Europees verband. Nederland kent sinds enkele jaren een beperkte bewaarplicht: bij mobiele telecommunicatie moeten aanbieders

[5] Zie *Kamerstukken II* 2003/04, 29 441, nr. 3, p. 8.
[6] Zie algemeen: <http://www.bof.nl/verkeersgegevens.html>, <http://www.xs4all.nl/nieuws/pdf/verslag_workshop.pdf>.

drie maanden gegevens bewaren welk nummer op welk tijdstip vanuit welk basisstation belde.
Nu wordt echter hard gewerkt aan een algemene, veel grootschaliger bewaarplicht. Binnen de EU wordt, vooral op aandrang van enkele lidstaten en met een krachtige wind in de rug sinds de aanslagen van 11 september 2001, een kaderbesluit overwogen dat lidstaten zou verplichten bewaring te eisen van alle verkeersgegevens gedurende één tot drie jaar.[7] Daarbij gaat het om de vastlegging en het behoud van gegevens die louter voor strafrechtelijke doeleinden moeten worden opgeslagen voor de toekomst, ongeacht of de aanbieder ze om zakelijke redenen al (even) opslaat of wil bewaren.
Voor de reikwijdte van zo'n bewaarplicht zal veel afhangen van de precieze invulling: welke gegevens moeten worden bewaard, en bij welke soorten telecommunicatie? Worden bijvoorbeeld aanbieders van mobiele telecommunicatie verplicht om telefoons die in de paraatstand staan, te volgen en om de 10 minuten vast te leggen in welke cel de mobiele telefoon zich bevindt? Worden Internetaanbieders verplicht om bij te houden welke weblocaties iemand precies bezoekt, inclusief alle subpagina's?
Een belangrijke vraag daarbij is ook hoe dit technisch en organisatorisch zal worden uitgevoerd. Het is allerminst zeker of telecomaanbieders technisch wel in staat zullen zijn al die gegevens vast te leggen. Een medewerker van XS4ALL berekende bijvoorbeeld dat als deze aanbieder alle verkeersstromen van en naar hun abonnees zouden moeten bijhouden, dit een slordige 600 dvd's per uur zou kosten. En als in al die vastgelegde gegevens dan een vraag zou komen welke berichten Mohammed op 28 januari 2004 had verstuurd, was volgens hem 'het zoeken naar een speld in een hooiberg nog een eufemisme'.[8] Los van de praktische kant is in Nederland ook de nodige kritiek geüit op de voorstellen voor een bewaarplicht vanuit principiële overwegingen.[9]
Het belangrijkste bezwaar acht ik dat hiermee de opsporing van strafbare feiten een andere rol gaat spelen in de maatschappij dan voorheen: justitie neemt geen genoegen met het zoeken naar voorhanden bewijsmateriaal, maar dwingt de samenleving haar processen zodanig in te richten dat justitie – als het ooit nodig mocht zijn – makkelijker aan bewijsmateriaal kan komen. Daarmee wordt de samenleving een instrument om opsporing mogelijk te maken, in plaats van andersom.

4. DNA-onderzoek[10]

4.1. DNA-databank

Op 16 september 2004 werd de wet DNA-onderzoek bij veroordeelden aangenomen.[11] Deze wet maakt het mogelijk om celmateriaal af te nemen van personen die veroordeeld zijn voor een misdrijf waarvoor voorlopige hechtenis is toegelaten (ex art. 67 lid 1 Sv). Met dit celmateriaal kan een DNA-profiel worden bepaald, dat dan aan de landelijke DNA-databank wordt toegevoegd. Het idee achter deze wet is dat hierdoor de kans zal toenemen dat in de toekomst sporenmateriaal

[7] *Draft Framework Decision on the retention of data (...) for the purpose of prevention, investigation, detection and prosecution of crime and criminal offences including terrorism*, 28 april 2004, beschikbaar op <http://register.consilium.eu.int/pdf/en/04/st08/st08958.en04.pdf>.
[8] Simon Hania, op de workshop Bewaarplicht verkeersgegevens, 24 september 2004.
[9] Zie bijvoorbeeld A. Patijn, 'Verplichte opslag van verkeersgegevens', *Computerrecht* 2003/2, p. 134-137, A.H. Ekker, 'Bewaarplicht verkeersgegevens veroorzaakt digitale boterberg', *I&I* 2002/5, p. 2-3, en B.J. Koops, *Strafvorderlijk onderzoek van (tele)communicatie 1838-2002. Het grensvlak tussen opsporing en privacy*, Deventer: Kluwer 2002, p. 131-139.
[10] Over DNA-onderzoek in strafzaken is sinds november 2003 een proefschrift in bewerking genomen door mr. Merel Prinsen, in het kader van een Tilburgs onderzoeksproject naar schuivende machtsverhoudingen.
[11] Stb. 2004, 465.

dat bij een misdrijf wordt aangetroffen, in verband wordt gebracht met een bekende (recidiverende) persoon.
In oktober 2004 zaten ruim 5000 profielen van personen in de databank;[12] de verwachting is dat dit aantal nu snel zal gaan groeien. De nieuwe wet maakt immers DNA-profilering mogelijk bij alle veroordeelden voor een 67-lid-1-misdrijf, ongeacht de strafmaat in het concrete geval. Iemand die een pak melk steelt uit de supermarkt en daarvoor geldboete krijgt opgelegd, kan ook in de databank terechtkomen – op het misdrijf van diefstal staat immers vier jaren gevangenisstraf. De enige restrictie die de wet biedt is dat geen profiel wordt opgenomen van een veroordeelde indien "redelijkerwijs aannemelijk is dat het bepalen en verwerken van zijn DNA-profiel gelet op de aard van het misdrijf of de bijzondere omstandigheden waaronder het misdrijf is gepleegd niet van betekenis zal kunnen zijn voor de voorkoming, opsporing, vervolging en berechting van strafbare feiten van de veroordeelde". Dat betekent dat bij delicten waarbij DNA naar verwachting geen rol zal spelen, ook geen DNA-profiel zal worden aangelegd; de memorie van toelichting noemt daarbij meineed en valsheid in geschrifte. Bij de opsporing van dergelijke misdrijven vindt immers ook geen DNA-onderzoek plaats.[13] Maar zelfs dat kan gaan veranderen: het is tegenwoordig mogelijk om DNA-sporen te vinden op brieven, sigarettenpeuken en drinkglazen, en dat maakt het mogelijk dat bij vele soorten misdrijven DNA een rol kan gaan spelen – ook bij bijvoorbeeld dreigbrieven en vervalste waardepapieren.
In Nederland zijn we met de DNA-databank nog bepaald niet zo ver als het Verenigd Koninkrijk. Daar worden niet alleen van veel veroordeelden DNA-profielen opgeslagen, maar ook van personen die verdacht zijn geweest van enig misdrijf – ongeacht of het misdrijf iets met DNA-opsporing te maken heeft en ongeacht of zij vervolgens vrijgesproken zijn.[14] De nieuwe Nederlandse wet zou een stap op weg kunnen zijn naar een dergelijke grootschalige databank (met als eindpunt wellicht een databank met een profiel van elke Nederlander?), maar dat hoeft niet per se. Wel is duidelijk dat DNA-opsporing een machtig middel is voor de overheid: aan een treffer in de DNA-databank wordt grote bewijswaarde toegekend. Aan de andere kant is het ook voor onschuldige burgers een machtig middel: als je DNA-profiel niet spoort met dat van het sporenmateriaal dat bij het misdrijf is aangetroffen, kun je sneller als onschuldige van verdenking worden uitgesloten (al heeft de Puttense moordzaak laten zien dat dit niet altijd het geval is).

4.2. DNA-persoonskenmerken[15]

DNA-onderzoek in strafzaken is van oudsher gericht op het vergelijken van DNA-profielen – juist daarom is de DNA-databank zo belangrijk. Sinds 2003 is echter een geheel nieuwe toepassing van DNA-onderzoek mogelijk: het afleiden van uiterlijke persoonskenmerken uit DNA-materiaal.[16] Dit zou de opsporing bij een onbekende verdachte op gang kunnen helpen: zoeken we een lange, blonde Fries, of moeten we eerder kijken naar tengere Midden-Afrikanen?
Voorlopig is deze wet beperkt tot het afleiden van twee kenmerken: geslacht en 'ras', zodat hooguit een compositietekening mogelijk is van een 'man uit Friesland' of een 'vrouw uit Zuidoost-Azië'. Veel zal de praktijk daar voorlopig niet mee opschieten. De wet is dan ook vooral op de toekomst gericht, waarbij de reikwijdte van de wet geleidelijk aan zal uitbreiden naarmate technisch meer mogelijk wordt en er meer persoonskenmerken bij AMvB aangewezen zullen worden voor het DNA-onderzoek.

[12] Zie <http://www.dnasporen.nl>.
[13] Kamerstukken 2002/03, 28 685, nr. 3, p. 10.
[14] Zie Statewatch, 'UK: Police can keep DNA of innocent people indefinitely', September 2004, <http://database.statewatch.org/unprotected/article.asp?aid=26055>.
[15] Zie uitgebreid B.J. Koops & M. Prinsen, 'Gezocht: blonde man uit Friesland. Verwonderpunten bij de wet DNA-onderzoek uiterlijk waarneembare persoonskenmerken' (in voorbereiding).
[16] Stb. 2003, 201, inwerkingtreding 1 september 2003, Stb. 2003, 312.

Verwacht wordt dat in de toekomst onder andere haarkleur, haarvorm, huidskleur, oogkleur en wellicht kenmerken als lichaamslengte uit DNA-materiaal kunnen worden afgeleid.
Het idee achter de nieuwe wet is om bij zaken met een onbekende verdachte waar nauwelijks een aanknopingspunt bestaat maar wel enig lichaamsmateriaal voorhanden is, via uiterlijk waarneembare kenmerken de opsporing op gang te brengen, met name via een compositietekening. Daarnaast kan de opsporing ook geholpen worden door bepaalde categorieën uit te sluiten; zo is het handig te weten dat bij de opsporing van een verkrachter bijvoorbeeld niet gelet hoeft te worden op allochtonen of donkerharigen, omdat het DNA-materiaal hoogstwaarschijnlijk van een blonde, inheemse Nederlander afkomstig is.
De wet is op diverse manieren beperkt: zo kunnen in de toekomst op te nemen kenmerken slechts vanaf de geboorte zichtbare uiterlijke kenmerken betreffen. Lichaamskenmerken die zich pas later openbaren, zoals wijnvlekken, worden dus uitgesloten, evenals innerlijke lichaamskenmerken en gedragskenmerken. Hierdoor wordt de reikwijdte van de wet behoorlijk ingeperkt en kan men hier niet echt spreken van een grote machtstoename bij de overheid.

5. Futuristische scantechnieken[17]

Om naast de recent ingevoerde en momenteel voorgestelde wetten ook een indruk te geven van wat ons in de toekomst te wachten staat, geef ik tot slot nog een beeld van enkele futuristische technieken. Deze klinken weliswaar nu nog vaak als *science fiction*, maar de techniek ontwikkelt zich sneller dan menigeen denkt.
Het huis wordt steeds elektronischer en wordt langzaamaan ingebed in een intern en extern computernetwerk, waarbij apparaten als koelkast en wasmachine naadloos (en draadloos) zijn opgenomen en zijn te bedienen via het Internet. Hiermee zal de scheiding tussen huis en buitenwereld vervagen en zal bijvoorbeeld een hacker van buitenaf in de koelkast kunnen 'kijken'. Daarbij komt dat ook de techniek om straling op te vangen steeds verfijnt, en bovendien zenden steeds meer apparaten in het huis via draadloze verbindingen straling uit, zodat straling van draadloze toetsenborden en huiscamera's (zoals *nannycams*) van buitenaf op te vangen is. Ook de observatie met infraroodapparatuur om warmtebronnen (zoals hennepkwekerijen of aan te houden personen) te lokaliseren zal belangrijker gaan worden. Door al dergelijke technieken wordt de woning dan langzaamaan transparant: de muren en gordijnen beschermen het huis niet langer tegen pottenkijkers.
Een andere ontwikkeling is dat steeds meer apparaten – maar uiteindelijk ook mensen zelf – zullen worden uitgerust met chips. Allerlei goederen zullen worden uitgerust met RFID-chips: een soort nieuwe streepjescode die op korte afstand automatisch uitleesbaar is, waarmee bijvoorbeeld winkeldiefstal kan worden voorkomen. Maar ook schijnt de Mexicaanse Minister van Justitie bij zichzelf en 160 medewerkers al een chip hebben laten implanteren die hen toegang geeft tot beveiligde ruimtes in het ministerie;[18] de Baja Beach Club kreeg veel gratis publiciteit door schaars geklede bezoekers een implantaat te geven waarmee zij kunnen betalen. Dit roept de nodige vragen op in hoeverre justitie de bevoegdheid heeft (of moet krijgen) om dergelijke chips op afstand heimelijk uit te lezen.
Een ander voorbeeld zijn geavanceerde camera's die – volgens sommigen – als een radarhuidscanner alle anatomische details tot een millimeter nauwkeurig kunnen registreren, waardoor het mogelijk wordt 'to "see through a person's clothing with such accuracy that it can scan someone standing on the street and detect the

[17] Zie uitgebreid Bert-Jaap Koops, Hanneke van Schooten & Merel Prinsen (2004), *Recht naar binnen kijken. Een toekomstverkenning van huisrecht, lichamelijke integriteit en nieuwe opsporingstechnieken*, Den Haag: Sdu 2004, ITeR-reeks deel 70, 221 p.
[18] Associated Press, 'Update 4: Chip Implanted in Mexico Judicial Workers', 14 juli 2004, beschikbaar op <http://www.forbes.com/business/manufacturing/feeds/ap/2004/07/14/ap1456551.html>.

diameter of a woman's nipples, or whether a man has been circumcised."'[19]
Daarnaast komen er camera's met gezichts- en gedragsherkenning, waarmee bij een demonstratie bekende raddraaiers of onbekende maar zich agressief gedragende betogers automatisch kunnen worden gelocaliseerd.
Dergelijke ontwikkelingen rond de woning en het menselijk lichaam roepen fundamentele vragen op in hoeverre justitie 'naar binnen mag kijken'. Voor een belangrijk deel zou justitie de bevoegdheid tot stelselmatige observatie kunnen inzetten om chips op afstand uit te lezen, slimme camera's te gebruiken die door kleding heenkijken, en gezichtsherkenning toe te passen. Maar in de huidige wet is stelselmatige observatie (art. 126g/o Sv) een relatief lichte bevoegdheid, die de officier van justitie kan uitoefenen bij verdenking van willekeurig welk misdrijf. Biedt dat de overheid – door de toenemende technische ontwikkelingen – niet automatisch meer macht dan waar de wetgever in 2000, toen deze nog absoluut niet dacht aan futuristische scantechnieken, toe heeft besloten?

6. Conclusie

Als we al deze ontwikkelingen in ogenschouw nemen, wat kunnen we dan concluderen bij de vraag of de overheid niet té machtig wordt bij bewijsvergaring door middel van techniek?
Laat ik vooropstellen dat ik in de beperkte ruimte van dit artikel geen aandacht heb besteed aan de andere kant van de machtsstrijd: de toenemende technische mogelijkheden voor misdadigers om te ontsnappen aan justitiële waarneming (bijvoorbeeld via gegevensversleuteling, steganografie – het verbergen van boodschappen in plaatjes, gedistribueerde gegevensopslag in het buitenland, *peer-to-peer*-netwerken en Internettelefonie). Want het is juist die kant van de medaille die de overheid vaak gebruikt als argument om nieuwe of uitgebreidere bevoegdheden te creëren. Justitie moet "bijblijven in de wapenwedloop met de georganiseerde misdaad", heet het dan.
Het is moeilijk om een oordeel te geven over de juistheid van een dergelijke bewering – en over de noodzaak om steeds weer ruimere bevoegdheden te scheppen. Want het techniekgebruik door misdadigers is vaak onzichtbaar, maar vooral blijft het vaak onduidelijk waarom de huidige bevoegdheden van justitie te kort schieten. Mijn indruk is dat het meestal eerder praktische of organisatorische beperkingen zijn waardoor de opsporing tekortschiet – bijvoorbeeld omdat er onvoldoende technisch opgeleide opsporingsambtenaren beschikbaar zijn – dan dat de wetgeving te beperkt is. Integendeel, sinds de Wet bijzondere opsporingsbevoegdheden (Wet BOB) uit 2000 is het opsporingsarsenaal al aan de ruime kant. De hierboven behandelde uitbreidingen versterken daarom wel de indruk dat de overheid steeds machtiger wordt.
Dat brengt mij op de belangrijkste boodschap van dit artikel: de machtsstrijd tussen georganiseerde, technisch onderlegde misdadigers en de overheid die voortdurend bevoegdheden uitbreidt om 'bij te blijven', kan misschien wel gezien worden als een machtsstrijd die in zekere mate onvermijdelijk is en die gevoerd moet worden. Wellicht is dat ook een per definitie onbesliste strijd.
De vraag is dan ook eigenlijk niet zozeer wie de machtsstrijd wint, maar wie verliest. Want het is de burger die van dat alles de dupe lijkt te worden: zij is de huilende derde. De bevoegdheden gaan namelijk in toenemende mate ten koste van de relatieve onzichtbaarheid van onschuldige burgers voor justitie. Sinds de wet BOB kunnen tal van bevoegdheden ook worden uitgeoefend tegenover burgers, en met de

[19] Judy Jones, 'Look Ahead to the Year 2000: Electronic Arm Of The Law Is Getting More High-Tech', *Courier Journal* (Louisville, KY) 19 oktober 1999, geciteerd in Michael Froomkin, 'The Death of Privacy?', *Stanford Law Review* May 2000, p. 1461-1543, <http://personal.law.miami.edu/~froomkin/articles/privacy-deathof.pdf>, p. 1501.

hierboven behandelde bevoegdheden komen burgers nog meer – en steeds scherper – in beeld van justitie. Dat betekent niet per se een verslechtering van fundamentele rechtsgoederen van de burger, zoals privacy, maar het gevaar dreigt wel dat burgers meer in aanraking komen met justitie en in het verlengde daarvan – onterecht – in het maatschappelijk verkeer worden geassocieerd met kwalijke zaken, onder het niet uit te roeien motto “waar rook is moet vuur zijn”.
Buruma heeft recentelijk gewaarschuwd voor het steeds meer vergaren en koppelen van gegevens in justitiële sfeer wanneer dat leidt tot het ontstaan van virtuele beelden van een persoon, waardoor die persoon onjuist wordt bejegend of behandeld.[20] Dezelfde redenering gaat op voor andere onderdelen van de privacy van burgers: hun huisrecht, lichamelijke integriteit en recht op vertrouwelijke communicatie. De tendens is dat de overheid een steeds beter beeld kan krijgen van alle aspecten van het persoonlijke leven van burgers, en dat geeft de overheid meer macht dan voorheen om die burgers – binnen of buiten de strafvordering – te behandelen op basis van het aldus ontstane beeld. Zal de overheid met voldoende terughoudendheid die macht gaan uitoefenen? Ik ben daar niet gerust op, en hoop in elk geval dat de wetgever tegenover de ‘stilzwijgend uitdijende opsporingsvergaarbak’[21] ook machtsbeperkingen gaat zetten. Twee waarborgen zijn daarbij cruciaal om de macht te beperken: doelbinding (het bepalen dat met opsporingsbevoegdheden vergaarde informatie alleen voor strafvordering kan worden gebruikt, en niet bijvoorbeeld bij vergunningverlening of belastingheffing) en controle: het vormgeven van adequaat toezicht op de uitoefening van bevoegdheden.[22] Alleen met expliciete en effectieve rechtswaarborgen kan de toenemende macht van de overheid ten opzichte van de burger in goede banen worden geleid.

[20] Y. Buruma, ‘Acht nieuwe wetten: de zin en onzin van gegevensbescherming’, *DD* 2004, 51.
[21] Aldus Corien Prins in *Nederlands Juristenblad* 2004 nr. 16.
[22] Vgl. de *Opinion of the Europol, Eurojust, Schengen and Customs Joint Supervisory Authorities presented to the House of Lords (...) for their inquiry into EU counter-terrorism activities*, Brussels 28 September 2004, <http://www.cbpweb.nl/downloads_overig/okt2004_opinies_gcas.pdf>: ‘The processing of personal data on the scale proposed (often involving the processing of information on those who are not suspected of any crime) requires adequate legal safeguards such as *purpose restriction*, with *supervision* to ensure that there is compliance with legal instruments’ (mijn cursivering).