Technology Assessment

Kansen en risico's van moderne opsporingsmethoden

Discussienotitie expertbijeenkomst Gegevensbescherming

Oktober 2008

Geert Munnichs, Anne Kets & Paul Breitbarth

Rathenau Instituut

Kansen en risico's van moderne opsporingsmethoden

Discussienotitie expertbijeenkomst Gegevensbescherming

Auteurs
Geert Munnichs – Rathenau Instituut
Anne Kets – Rathenau Instituut
Paul Breitbarth – Eerste Kamer der Staten-Generaal, afdeling Inhoudelijke Ondersteuning

Deze publicatie is een licht gewijzigde versie van de discussienotitie zoals geschreven voor de expertbijeenkomst over gegevensbescherming van 20 maart 2008. De bijeenkomst werd georganiseerd door het Rathenau Instituut samen met de vaste commissie voor Justitie van de Eerste Kamer der Staten-Generaal.

Inhoudsopgave

Inleiding

Deze discussienotitie behandelt het onderwerp gegevensbescherming binnen de context van veiligheid en opsporing. Ze is het resultaat van een samenwerking tussen de commissie Justitie van de Eerste Kamer en het Rathenau Instituut. De notitie vormt het uitgangsmateriaal voor een expertbijeenkomst die op 20 maart 2008 wordt gehouden. Aan de hand van drie casusposities worden aandachtspunten geformuleerd voor het debat over veiligheid en gegevensbescherming. Doel van de bijeenkomst is criteria te identificeren aan de hand waarvan binnen het wetgevingsdebat privacy- en veiligheidsbelangen op evenwichtige wijze kunnen worden gewogen.

Veiligheid staat hoog op de politieke en maatschappelijke agenda. Dat is in belangrijke mate een gevolg van de terreuraanslagen aan het begin van de 21e eeuw, maar gaat terug op de opkomst van georganiseerde misdaad halverwege de jaren tachtig van de vorige eeuw. In de strijd tegen misdaad en terreur zijn de afgelopen jaren de bevoegdheden van de opsporings-, inlichtingen- en veiligheidsdiensten drastisch uitgebreid. Deze bevoegdheidsuitbreidingen zijn mede ingegeven door de steeds grotere beschikbaarheid van technologische middelen die voor opsporings- en veiligheidsdoeleinden kunnen worden ingezet.

De belangrijkste en meest vernieuwende trend betreft het toenemende gebruik van gedigitaliseerde gegevens voor opsporings- en veiligheidsdoeleinden. Door de voortschrijdende digitalisering worden gegevensbestanden niet alleen beter toegankelijk, maar kunnen bovendien aan elkaar worden gekoppeld en door middel van computerprogramma’s worden geanalyseerd (datamining). Dat geldt tevens voor Europees niveau. Van personen die een visum nodig hebben voor de Europese Unie of die asiel aanvragen, worden de gegevens opgeslagen in en gecontroleerd met behulp van grote databanken. Deze bestanden worden in toenemende mate ook opengesteld voor opsporingsdoeleinden.

Ook elders binnen het opsporingsapparaat valt een groeiende inzet van technologie waar te nemen: toezichtcamera’s, het forensisch gebruik van DNA-profielen, het aftappen van telecommunicatie, de invoering van het biometrisch paspoort, etc. De digitalisering en koppeling van bestanden leiden ook bij deze toepassingen tot bredere en intensievere vormen van surveillance. Zo kunnen camerabeelden worden gekoppeld aan databestanden met kentekenplaten of kunnen in DNA-databanken opgeslagen gegevens worden uitgewisseld met andere landen. Deze ontwikkelingen gelden zowel voor het nationale als het internationale niveau. Zie onder meer de steeds intensievere politiële en justitiële samenwerking tussen de EU-lidstaten of de uitwisseling van passagiersgegevens met de Verenigde Staten.

Kansen en risico’s

Het toenemende gebruik van technologie moet de criminaliteit bestrijden en nieuwe terreuraanslagen voorkomen – en daarmee de veiligheid verhogen. Over het algemeen kan worden gesteld dat binnen het opsporings- en veiligheidsapparaat hoge verwachtingen bestaan van de mogelijkheden die technologie biedt. Zie bijvoorbeeld de volgende uitspraak van Harm Brouwer, voorzitter van het College van procureurs-generaal: “Hoe intensiever bedrijven gebruik gaan maken van RFID, des te meer mogelijkheden er ontstaan voor de opsporing.” En ook de invoering van de

OV-chipkaart kan volgens hem opsporingsdoeleinden dienen: "Die [OV-chipkaart] zal ons de mogelijkheid bieden (…), uit te vinden wanneer een verdachte op de trein is gestapt of waar en wanneer de OV-kaart uit een geroofde handtas langs een detectiepoortje is gegaan. Naarmate meer functies aan de kaart worden gekoppeld, kan ook meer informatie beschikbaar komen, bijvoorbeeld over het betalingsverkeer van de kaarthouder" (Rathenau Instituut 2007).

De inzet van technologie roept echter ook vragen op. Zo is het vaak onduidelijk wat de effectiviteit is van de veiligheidsmaatregelen: leiden ze inderdaad tot een betere bestrijding van de misdaad en het voorkomen van nieuwe terreuraanslagen? Tevens kunnen kanttekeningen worden geplaatst bij de ermee gemoeide kosten en bij de betrouwbaarheid van de uitkomsten. Ook is het de vraag wat voor gevolgen de uitgebreide opsporingsbevoegdheden hebben voor de rechtsbescherming van de burger en welke verweermogelijkheden burgers hebben als zij ten onrechte als verdachte worden aangemerkt.

In deze discussienotitie wordt nader ingegaan op het gebruik van een aantal nieuwe technologieën voor opsporings- en veiligheidsdoeleinden en daaraan gerelateerde bevoegdheidsuitbreidingen. We willen daarmee meer zicht krijgen op de issues die relevant zijn voor de discussie over het veiligheidsbeleid. Daarvoor willen we zowel ingaan op de kansen die de nieuwe technologieën bieden als op de mogelijke risico's die daarmee gepaard gaan. Door aan beide aspecten aandacht te besteden, willen we een doordachte oordeelsvorming mogelijk maken over de gewenste balans tussen veiligheid en privacy (vergelijk Muller, Kummeling & Bron 2007). Uiteindelijk doel is om de parlementariërs te voorzien van een aantal handvatten die zij kunnen gebruiken bij de weging van (toekomstige) wetgeving die de hierboven aangehaalde bevoegdheden regelt.

Casusposities

Aan de hand van drie casusposities zal het gebruik van nieuwe technologieën voor opsporings- en veiligheidsdoeleinden worden besproken:

- Gebruik van databanken
- DNA-onderzoek
- Cameratoezicht

Het gebruik van databanken vormt het belangrijkste thema. Met de twee andere thema's, DNA-onderzoek en cameratoezicht, willen we nagaan of er meer algemene patronen of vanzelfsprekendheden kunnen worden achterhaald in de omgang met technologie vanuit veiligheidsperspectief. Daarmee hopen we nog beter zicht te krijgen op de issues die ons in staat stellen om beide perspectieven – veiligheid én privacy – met elkaar te verbinden.

Gebruik van databanken

Informatiegestuurde opsporing

Inlichtingen- en opsporingsdiensten maken in toenemende mate gebruik van allerlei gedigitaliseerde databestanden. Dat geldt niet alleen voor eigen opsporingsregisters, maar tevens voor databestanden van derden en voor de bestanden van inlichtingen- en opsporingsdiensten van andere EU-lidstaten en derde landen.

Voor de situatie in Nederland is in dit verband de Wet bevoegdheden vorderen gegevens (2006)[1] van groot belang. Met deze wet krijgen politie en justitie in principe toegang tot de databestanden van andere overheidsorganisaties alsook van private organisaties. Volgens deze wet mag een opsporingsambtenaar identificerende gegevens vorderen. Hieronder vallen gegevens over naam, adres, woonplaats, geboortedatum, geslacht, rekeningnummers en andere administratieve kenmerken. Daarnaast mag een officier van justitie ook andere gegevens vorderen. In dringende gevallen mag hij bovendien 'gevoelige' gegevens vorderen, dat wil zeggen persoonsgegevens betreffende iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven of lidmaatschap van een vakvereniging. De officier heeft hiertoe voorafgaande machtiging door de rechter-commissaris nodig. Identificerende gegevens kunnen worden gevorderd als sprake is van verdenking van een misdrijf. De overige gegevens kunnen worden gevorderd bij verdenking van een misdrijf waarvoor voorlopige hechtenis is toegelaten en dat een ernstige inbreuk op de rechtsorde oplevert. Hieronder vallen bijvoorbeeld terroristische misdrijven en ernstige misdrijven in georganiseerd verband (Vedder et al. 2007). Andere relevante maatregelen zijn de Europese Richtlijn Dataretentie (2006)[2], de Wet politiegegevens (2007)[3] en het wetsvoorstel Wijziging van de Wet op de inlichtingen- en veiligheidsdiensten (2007)[4].

Het groeiende belang van gedigitaliseerde informatie vormt de belangrijkste trend op het gebied van opsporing en veiligheid. Dat geldt zowel voor de inlichtingen- en veiligheidsdiensten als in toenemende mate ook voor het opsporingsapparaat. Onder de noemer van 'informatiegestuurde opsporing' en 'nodale oriëntatie' gaat binnen het opsporingsapparaat steeds meer aandacht uit naar het gebruik van databestanden. Zo pleit commissaris Jan Boersma van de Nationale Recherche voor het koppelen van politieregisters, overheidsbestanden zoals die van de fiscus, het kadaster en de Rijksdienst voor het wegverkeer, externe bestanden van de Kamer van Koophandel en bronnen op internet waar criminelen sporen achterlaten (de Volkskrant 5 november 2007). Volgens deze gedachtegang is het gebruik van ICT nodig om crimineel gedrag transparant te maken. Alleen op die manier kan volgens Boersma de politie aansluiting vinden bij de huidige netwerksamenleving, die zich niet langer alleen in de 'reële' maar in toenemende mate ook in de virtuele wereld afspeelt (Boersma 2007; vergelijk Raad van Hoofdcommissarissen 2004). Deze gedachtegang vormt ook een belangrijke beweegreden voor de politiële en justitiële bevoegdheidsuitbreidingen van de

[1] Stb. 2005, 390

[2] Richtlijn 2006/24/EG, PbEU L105 van 13 april 2006; zie ook Kamerstukken 31145

[3] Stb. 2007, 300

[4] Kamerstukken 30553

afgelopen jaren. Omdat criminele netwerken en terreurgroepen meer en meer gebruikmaken van de mogelijkheden die ICT biedt, kunnen politie en justitie moeilijk achterblijven (Koops 2006).

Een belangrijk kenmerk van informatiegestuurde opsporing is haar proactieve karakter: het wordt preventief ingezet om misdrijven en aanslagen te voorkomen. Dit gaat gepaard met omslag in denken over verdacht gedrag. Terwijl voorheen alleen onderzoek kon worden verricht als daar concrete aanleiding voor bestond, richt het vizier zich nu meer en meer op potentieel verdacht gedrag. Door databestanden aan de hand van risicoprofielen te analyseren (datamining) kunnen 'patroonafwijkingen' worden gesignaleerd. Ook niet-verdachte personen kunnen daarmee betrokken worden bij opsporingsonderzoek – simpelweg omdat ze in een bepaald risicoprofiel passen (Vedder et al. 2007).

Kanttekeningen

In haar rapport 'Data voor daadkracht' (2007) onderwerpt de commissie-Bosma de trend van informatiegestuurde opsporing aan inspectie. De commissie is van mening dat informatiegestuurd optreden van de politie in tweeërlei opzicht in de kinderschoenen staat. Aan de ene kant worden de potenties ervan bij lange na niet gerealiseerd – onder meer omdat bij veel opsporings- en veiligheidsinstanties weerstand bestaat tegen het uitwisselen van data met andere diensten. Aan de andere kant omdat op een weinig systematische, veelal ongerichte wijze informatie wordt verzameld, waarbij bovendien weinig aandacht bestaat voor essentiële voorwaarden als het kunnen beschikken over correcte data en een adequate interpretatie en analyse van die data.

Uit internationaal vergelijkend onderzoek van de WODC blijkt dat de tendens om steeds meer bestanden aan elkaar te koppelen in landen als de Verenigde Staten of Duitsland vooralsnog vooral leidt tot een overvloed aan data, vaak van matige kwaliteit, waaruit moeilijk patronen zijn te halen (Neve et al. 2006). Dit beeld lijkt te worden bevestigd door een recente lezing van procureur-generaal Han Moraal die stelt dat de 'explosie' aan informatie weliswaar veel kansen biedt voor het opsporingsapparaat, maar contraproductief dreigt uit te pakken doordat politie en justitie overspoeld worden door een overdosis aan informatie (Staatscourant 14 september 2007).

Het WODC-rapport maakt melding van een 'watch list' van het Amerikaanse State Department met informatie over 100.000 mogelijke terreurverdachten. The Washington Post maakte vorig jaar melding van het bestaan van een antiterreurlijst met maar liefst 435.000 potentiële verdachten. Deze getallen roepen de vraag op hoe werkbaar dergelijke lijsten zijn. Hierbij moet worden bedacht dat computeranalyses 'platte' data opleveren, die losgekoppeld zijn van hun oorspronkelijke context. Een zinvol gebruik van deze data voor opsporingsdoelen vergt een adequate interpretatie ervan – waarvoor we nog steeds zijn aangewezen op 'human intelligence'.

De commissie-Bosma wijst daarnaast op het probleem van bestandsvervuiling. Vervuilde data kunnen leiden tot verkeerde uitkomsten, waardoor ten onrechte bepaalde personen als verdachte worden aangemerkt. Dit risico op 'vals positieven' is allesbehalve denkbeeldig, als bedacht wordt dat in de Gemeentelijke Basisadministratie van Amsterdam meer dan zeven procent van de adressen niet klopt. Spelfouten, naamsverwisselingen of verschillende schrijfwijzen van Arabische namen blijken een notoire bron van bestandsvervuiling.

Een verder aandachtspunt betreft de beveiliging van databestanden. Recente incidenten in Engeland (waar bij diverse incidenten persoonsgegevens van miljoenen Britten op straat kwamen te liggen) en Nederland (waar de OV-chipkaart werd gehackt) wijzen daarop. De commissie-Bosma vermeldt dat in de VS in 2003 meer dan drie miljoen mensen slachtoffer zijn geworden van identiteitsdiefstal. Govcert wijst in een recent rapport tevens op het groeiende probleem van *cybercrime* (Govcert 2007). Jacobs en Jochems (2007) wezen er onlangs op dat in Nederland de beschermingsmaatregelen voor DigiD onvoldoende zijn om identiteitsfraude te voorkomen. Dit roept de vraag op hoe voorkomen kan worden dat kwaadwillenden met behulp van de digitale identiteit van iemand anders misdaden begaan. Ook kan de vraag worden gesteld of de overheid bij de invoering van het Burgerservicenummer voldoende waarborgen inbouwt om identiteitsfraude te voorkomen. Naarmate meer (externe) databestanden gebruikt worden voor opsporingsdoeleinden, vormt identiteitsdiefstal ook vanuit opsporingsperspectief een groeiend probleem.

Dit laatste wordt nog eens versterkt door de continue technologische wedloop die gaande is tussen het opsporings- en veiligheidsapparaat aan de ene kant en de georganiseerde misdaad en terreurgroepen aan de andere kant. Niet alleen worden er steeds verfijndere methoden ontwikkeld voor identiteitsfraude, tevens kunnen kwaadwillenden bijvoorbeeld door middel van encryptie ontsnappen aan het vizier van politie en justitie (Koops 2006).

Aan de andere kant blijkt in de praktijk de identificatie van verdachte personen over het algemeen niet het grootste probleem. Opsporings- en veiligheidsdiensten weten vaak goed welke personen of groepen extra in de gaten gehouden moeten worden. Het probleem schuilt veelal in het aandragen van voldoende bewijsvoering om iemand daadwerkelijk op te kunnen pakken. Zie het voorbeeld van Mohammed B., die al langere tijd voor zijn aanslag in de gaten werd gehouden. Ook hier geldt dat adequate analyse en interpretatie van de beschikbare informatie van groot belang zijn.

De commissie-Bosma wijst daarnaast op de tekortschietende rechtsbescherming van burgers. De uitbreiding van de bevoegdheden en technologische mogelijkheden van politie en justitie voor data-analyse gaat volgens de commissie niet gelijk op met waarborgen voor de persoonlijke levenssfeer van burgers op wie geen verdenking berust. Het gevaar bestaat dat mensen geboekstaafd worden als staatsgevaarlijk individu of potentieel terrorist zonder dat ze mogelijkheden hebben om zich daartegen te verweren. Vaak zullen ze niet eens weten dat ze een dergelijk profiel hebben (vergelijk Vedder et al. 2007).

Ten slotte wijst de commissie-Bosma erop dat de informatiegestuurde opsporing gepaard gaat met een grote belasting van instanties en bedrijven die informatie moeten aanleveren. Om enkele cijfers te noemen: het Meldpunt Ongebruikelijke Transacties heeft in 2005 ruim 180.000 meldingen gedaan (waarvan overigens maar 130 gevallen tot een rechtszaak hebben geleid); het Nederlandse bankwezen is voor informatievoorziening in het kader van criminaliteits- en terrorismebestrijding op jaarbasis 480 miljoen euro kwijt, welk bedrag mogelijk teruggebracht kan worden naar 320 miljoen; het aantal bevragingen bij het CIOT over gebruikersgegevens voor telefoniediensten laat een sterk stijgende lijn zien: van 722.000 in 2003 tot meer dan 1,8 miljoen in 2006. Ook kan worden gewezen op de klachten van telecomproviders

over de kosten die zij moeten maken om te kunnen voldoen aan de bewaarplicht voor telecommunicatiegegevens volgens de Europese Richtlijn Dataretentie.[5]

Europese ontwikkelingen

Ook op het niveau van de Europese Unie wordt in toenemende mate gebruikgemaakt van databanken om het personenverkeer van buitenaf te monitoren, vooral op het terrein van de justitiële en politiële samenwerking. Zonder naar volledigheid te streven, worden hier kort enkele datasystemen besproken.

Het Schengen Informatiesysteem (SIS) wordt gebruikt ter ondersteuning van de bewaking van de buitengrenzen van het Schengengebied en ter bevordering van het vrije verkeer van personen binnen het gebied. In het systeem worden personen, voertuigen en andere goederen opgenomen die om een of andere reden gesignaleerd staan. Hierbij kan het gaan om ongewenst verklaarde vreemdelingen, maar ook om vermissingen. In een nieuwe versie (SIS II), die eind 2008 in gebruik moet worden genomen, zullen tevens biometrische kenmerken en foto's opgenomen worden. Vooral 'ongewenste vreemdelingen' staan geregistreerd – momenteel circa 750.000 (NRC Handelsblad 19 december 2007).

Het Visum Informatieysteem (VIS) is eveneens gekoppeld aan het Schengengebied. Vanwege het vrije verkeer van personen, hebben de Schengenlanden afgesproken een gezamenlijk visumbeleid te voeren. Visumplichtige inwoners van derde landen hebben daardoor de mogelijkheid één visum voor het hele gebied aan te vragen. De bij de visumaanvraag verstrekte informatie wordt in het VIS geregistreerd, ook indien een aanvraag wordt geweigerd of het visum wordt ingetrokken. De toegang tot het VIS is opgedeeld in verschillende categorieën. Zo hebben de douane en de asiel- en immigratiediensten enkel toegang tot die gegevens die voor hun werkzaamheden relevant zijn.

Eurodac is een registratiesysteem voor vingerafdrukken, dat onder meer wordt gebruikt om asielzoekers te identificeren, alsmede personen die bij de illegale overschrijding van een buitengrens van de EU zijn aangehouden. Door vingerafdrukken te vergelijken, kunnen de lidstaten nagaan of een asielzoeker of een vreemdeling die zich illegaal op het grondgebied bevindt, reeds een asielaanvraag heeft ingediend in een andere lidstaat en of een asielzoeker het grondgebied van de Unie onrechtmatig is binnengekomen.

Het Europol Informatiesysteem (EIS) wordt gebruikt voor de opslag en analyse van gegevens die door Europol worden gebruikt voor de uitoefening van zijn taak. Het systeem kan worden gekoppeld aan de informatiebestanden van de nationale rechtshandhavingsautoriteiten, maar mag niet in verbinding staan met andere geautomatiseerde gegevensbestanden. Toegang tot het EIS is voorbehouden aan gemachtigde personeelsleden van Europol en de nationale verbindingsofficieren.

Daarnaast is sprake van een toenemende uitwisseling tussen EU-lidstaten van nationale databestanden, zoals politieregisters of nationale DNA-databanken. Ook de Europese Richtlijn Dataretentie (2006) mag in dit verband niet ongenoemd blijven.

[5] Stb. 2007, 288

Deze richtlijn verplicht tot opslag van verkeersgegevens door telecommunicatie-bedrijven voor een periode van een half tot twee jaar. Het doel is om politie, justitie en inlichtingendiensten langer dan nu het geval is, in staat te stellen gegevens te kunnen vorderen (Vedder et al. 2007).

In navolging van de Verenigde Staten heeft de Europese Commissie onlangs het voorstel gedaan om luchtvaartmaatschappijen te verplichten gegevens (Passenger Name Records, PNR) van passagiers die op de EU vliegen door te spelen aan de nationale autoriteiten. De Nederlandse overheid is positief: “Op deze manier wordt de kans dat op het grondgebied van de Europese Unie terroristische aanslagen of ernstige misdrijven worden gepleegd kleiner en wordt de veiligheid vergroot”, aldus staatssecretaris Timmermans. In de toekomst wil Nederland ‘niet uitsluiten’ dat ook andere vervoerssectoren persoonsgegevens moeten gaan afstaan (Staatscourant 4 februari 2008).

Knelpunten

De grote hoeveelheid databanken die binnen de Europese Unie bestaat, roept diverse vragen op. Zo zijn de criteria voor registratie in het SIS weinig transparant. Over opname in het SIS beslissen de nationale autoriteiten, die daarvoor verschillende maatstaven hanteren (NRC Handelsblad 19 december 2007). Een tweede knelpunt vormt de betrouwbaarheid van de gegevens. Doordat vele instanties gegevens in de databanken kunnen invoeren, is lastig na te gaan hoe betrouwbaar deze gegevens zijn. Ook worden bepaalde categorieën gegevens niet in alle lidstaten op gelijke wijze geïmplementeerd.

Bovendien ontbreekt een uniform stelsel voor gegevensbescherming.[6] Elk systeem heeft eigen bepalingen met betrekking tot zaken als beveiliging en inzagerecht. Ook bestaat veel onduidelijkheid over de mogelijkheden voor doorgifte van informatie aan derden. Het toezicht op de verwerking van gegevens is in handen van een groot aantal instanties, al wordt in de Raad gesproken over het onderbrengen van het toezicht bij één instantie.

Over systemen als SIS, VIS en Eurodac merkt jurist Evelien Brouwer op: “Europa bouwt aan een grootschalig informatienetwerk dat stoelt op een heilig geloof in de effectiviteit en de kwaliteit van de verzamelde data. Dat is nogal naïef. De risico’s van onjuiste gegevensopslag worden juist steeds groter”. Ook valt er het nodige aan te merken op de rechtmatigheid van de SIS-gegevens. Volgens Brouwer bleek in Duitsland 20 procent van de onderzochte registraties uit 2004 gebaseerd op een onjuiste rechtsgrondslag (NRC Handelsblad 5 oktober 2007).

[6] Over de bescherming van persoonsgegevens verwerkt in het kader van de Europese politiële en justitiële samenwerking wordt sinds 2005 onderhandeld. Zie commissievoorstel COM(2005)475.

Aandachtspunten gebruik van databanken

Het gebruik van databanken voor opsporings- en veiligheidsdoeleinden roept de volgende vragen op:

- Hoe kan datamining het meest effectief worden ingezet voor opsporings- en veiligheidsdoeleinden? Is het instrument voldoende ontwikkeld voor preventief onderzoek naar potentieel verdacht gedrag?

- Hoe kunnen waarborgen worden ingebouwd om de risico's van slordig beheer, inbraak en identiteitsfraude te minimaliseren?

- Hoe kan worden gewaakt over de betrouwbaarheid van de opgeslagen data en kan – in het verlengde daarvan – worden voorkomen dat burgers als gevolg van bestandsvervuiling ten onrechte als (mogelijk) crimineel of terrorist worden aangemerkt?

- Welke maatregelen kunnen worden getroffen opdat burgers in beroep kunnen gaan tegen een onterechte verdachtmaking?

DNA-onderzoek

Sinds 1994 mag de rechter-commissaris in geval van zware misdrijven (waar een gevangenisstraf op staat van zes jaar of meer) en dringende noodzakelijkheid het bevel geven om bloed af te nemen van een verdachte. Met het voortschrijden van de DNA-technologie – waardoor ook uit wangslijm voldoende DNA-materiaal kan worden gehaald – wordt deze bevoegdheid verruimd. De wetgever acht het afnemen van wangslijm een kleinere inbreuk op de lichamelijke integriteit dan het afnemen van bloed. Sinds 2001 mag ook de officier van justitie het bevel geven tot afname van lichaamsmateriaal voor DNA-onderzoek. Bovendien mag DNA-onderzoek bij meer misdrijven worden uitgevoerd dan voorheen: grofweg misdrijven waarvoor een maximumstraf geldt van vier jaar of meer. Hieronder vallen vergrijpen als woninginbraak en winkeldiefstal.

De mogelijkheden van DNA-onderzoek zijn sindsdien verder uitgebreid. Ten eerste is de bevoegdheid geschapen om uit DNA-materiaal dat bij een misdrijf is gevonden uiterlijk waarneembare kenmerken af te leiden van de verdachte. Een tweede uitbreiding betreft het aanleggen en vullen van een DNA-databank. Hierin worden sinds de jaren negentig profielen bewaard van veroordeelde personen van wie DNA-materiaal is afgenomen. Omdat bij lang niet alle strafzaken DNA-onderzoek nodig of mogelijk is, blijft het aantal DNA-profielen in de databank beperkt. Dit verandert door genoemde wetswijziging. Door standaard een DNA-profiel op te slaan van ieder die wordt veroordeeld voor een misdrijf waarop een straf mogelijk is van vier jaar of meer, neemt het aantal opgeslagen profielen sterk toe: van 6.000 in 2004, bij de inwerkingtreding van de wet, tot 50.000 in februari 2008. Indien de verdenking vervalt, dient het Nederlands Forensisch Instituut (NFI), dat de databank beheert, het desbetreffende DNA-profiel uit de databank te verwijderen (Vedder et al. 2007).

Kansen en risico’s

In vergelijking met vingerafdrukken zijn DNA-sporen gemakkelijker te vinden, bevatten ze meer informatie en hebben ze een (veel) groter onderscheidend vermogen (Kruisbergen & De Poot 2007). Forensisch deskundige Broeders beschouwt de introductie van DNA- onderzoek voor identificatiedoeleinden als de belangrijkste forensische ontwikkeling van de 20e eeuw (Broeders 2006). Diverse betrokkenen koesteren dan ook grote verwachtingen van het gebruik van DNA-materiaal voor opsporingsdoeleinden: zie de nota van het ministerie van Justitie over het forensisch gebruik van DNA-onderzoek (2007) of het rapport van de Raad van Hoofdcommissarissen ‘Spelverdeler in de opsporing’ (2004). De Raad van Hoofdcommissarissen verwacht dat de rechtshandhaving de komende jaren ingrijpend zal worden beïnvloed door forensisch onderzoek. De verwachting is dat het oplossingspercentage van misdrijven fors kan worden opgeschroefd (NRC Handelsblad 18 maart 2005). Behalve binnen het opsporingsapparaat, bestaat ook binnen de rechterlijke macht en de advocatuur over het algemeen een groot vertrouwen in de betrouwbaarheid van DNA-bewijsvoering. Ietwat gechargeerd gesteld: “Een DNA-profiel liegt niet”.

Er kunnen echter ook kanttekeningen worden geplaatst bij het gebruik van DNA-sporen voor opsporingsonderzoek. Voor het doel van deze discussienotitie beperken we ons tot kwesties van de bewijskracht van DNA-materiaal, het nut van DNA-databanken en de positie van de burger.

Deskundigen geven aan dat DNA-onderzoek weliswaar een groot onderscheidend vermogen heeft, maar dat forensisch bewijs zelden honderd procent waterdicht is. DNA-materiaal kan hoogstens met zekerheid *uitsluiten* dat iemand op de plaats delict is geweest. DNA-profielen behoeven altijd nadere interpretatie. Dit hangt samen met het feit dat overeenkomsten tussen gevonden sporen en een DNA-profiel (die iemand tot een verdachte kunnen maken) moeilijker zijn vast te stellen dan verschillen (die iemand vrij kunnen pleiten). Interpretaties gaan daarbij altijd gepaard met bepaalde foutmarges, als gevolg van fouten bij de verwerking, verschrijvingen of vervuild DNA-materiaal. Bovendien bewijst een 'match' tussen DNA-sporen en een bepaald profiel niet dat de persoon in kwestie ook de feitelijke dader is. De relatie tussen spoor en delict is vaak onduidelijk – en behoeft nadere duiding. Zo kunnen inbrekers een dwaalspoor uitzetten door doelbewust DNA-materiaal van anderen achter te laten: in feite een vorm van identiteitsdiefstal. Om iemand aan te kunnen wijzen als dader van een misdrijf is dus altijd aanvullend bewijs nodig.

De voortschrijdende technologische mogelijkheden om ook gedeeltelijk, beschadigd of gemengd DNA-materiaal te kunnen analyseren, leiden niet zonder meer tot een grotere bewijskracht. Vanwege extra onzekerheden neemt bij deze mogelijkheden het belang van een adequate interpretatie alleen maar toe.

De onzekerheden die de bewijskracht van DNA-materiaal omgeven, blijken in de praktijk lastig te communiceren. Het ontbreekt opsporingsambtenaren en rechters over het algemeen aan voldoende kennis om forensisch bewijs goed te interpreteren. De neiging bestaat om te veel zekerheid toe te dichten aan DNA-bewijs. Forensisch wetenschapper Peter de Knijff ziet een steeds groter wordende kloof tussen de juridische en wetenschappelijke wereld. Hij pleit er dan ook voor dat rechters, advocaten en officieren van justitie in de toekomst over fundamentele basiskennis over forensisch DNA-onderzoek beschikken (NRC Handelsblad 17 maart 2004).

Daarnaast bestaat onduidelijkheid over het nut van grote DNA-databestanden. Aan de ene kant geldt dat hoe meer profielen een DNA-databank bevat, hoe groter de kans is dat het profiel van een dader van een misdrijf in het bestand voorkomt. Zo leidt in Engeland en Wales het grootschalig gebruik van DNA-materiaal tot een hoger oplossingspercentage van onder meer woninginbraken (Broeders 2005). Dat zegt echter nog niet alles over de effectiviteit daarvan. Aan de andere blijkt namelijk ook dat hoe groter een DNA-databank is, hoe groter de kans is op een 'mismatch' – op een vals positief resultaat. Dit laatste kan het gevolg zijn van bestandsvervuiling, maar hangt ook samen met de periode waarin gegevens worden bewaard. Hoe langer DNA-profielen van in het verleden veroordeelde personen worden bewaard, hoe groter de kans dat op een gegeven moment sporen van zo'n persoon op een plaats delict worden aangetroffen en hij als verdachte wordt aangemerkt, zonder dat hij iets met het delict te maken heeft. Hoe grootschaliger het onderzoek, hoe groter de kans op onterechte verdachtmakingen. Het wordt dan de vraag hoe het aantal 'matches' zich verhoudt tot het aantal 'mismatches'.

Over de effectiviteit van DNA-onderzoek zijn weinig cijfers bekend. Kruisbergen en De Poot (2007) wijzen erop dat de effectiviteit niet moet worden overschat. In Engeland en Wales, die wat DNA-onderzoek betreft internationaal vooroplopen, zou in het jaar 2002-2003 slechts 1,5% van de misdrijven dankzij DNA-onderzoek zijn opgehelderd.

Bij de vraag naar de effectiviteit van DNA-onderzoek zou tevens naar de vaak hoge kosten ervan moeten worden gekeken.

Hieraan gekoppeld is het de vraag met welk doel een DNA-databank wordt opgezet. Wordt DNA-onderzoek vooral ingezet met het oog op zwaardere misdrijven (moord, verkrachting, geweldpleging), of gaat het ook om zogeheten volumecriminaliteit (woninginbraak, diefstal)? In Nederland valt een trend waar te nemen om voor steeds lichtere vergrijpen DNA-afname van verdachten mogelijk te maken – tot aan winkeldiefstal toe. Behalve effectiviteitsvragen roept deze trend de vraag op 'waar de grens ligt' (vergelijk Vedder et al. 2007).

Met de groei van het aantal profielen in de DNA-databank neemt de urgentie toe van adequaat toezicht op de zuiverheid van het databestand. In dit verband is het opmerkelijk dat de wettelijke vernietigingsplicht slecht wordt nageleefd. Deze plicht houdt in dat het profiel van een verdachte vernietigd wordt zodra duidelijk wordt dat hij niet langer als verdachte kan worden aangemerkt. Burgers blijken er ook geen zicht op te hebben of hun profiel is vernietigd (Buiter et al. 2003).

Europese uitwisseling

In 2007 hebben de EU-ministers van Justitie en Binnenlandse Zaken een akkoord gesloten over het uitwisselen van DNA-informatie van verdachten en veroordeelden, in het kader van de bestrijding van grensoverschrijdende criminaliteit.[7] Ze breiden daarmee het Verdrag van Prüm[8] uit tot alle 27 landen van de Europese Unie. Volgens Europees privacytoezichthouder Peter Hustinx gaat deze uitbreiding te snel. Verschillende landen hanteren verschillende criteria voor opname in een DNA-bestand en houden er verschillende regimes voor gegevensbescherming op na. In deze situatie is het voor burgers onduidelijk hoe zij hun recht kunnen halen als ze ergens ten onrechte van worden verdacht (NRC Handelsblad 14 juni 2007).

Momenteel is een kaderbesluit bescherming persoonsgegevens in voorbereiding, dat minimumwaarborgen moet bieden voor het gebruik van gegevens bij politiële en justitiële samenwerking. Op het ontwerp kaderbesluit bestaat kritiek. Het maakt (ruime) uitzonderingen mogelijk op het beginsel van doelbinding. Bovendien mogen lidstaten zelf beslissen of ze gegevens die in het kader van de EU-samenwerking zijn verzameld of uitgewisseld, aan derde landen of internationale organisaties overdragen.

Aandachtspunten DNA-onderzoek

- De bewijskracht van DNA-onderzoek lijkt minder groot dan vaak wordt aangenomen. Dit roept de vraag op hoe binnen het opsporingsapparaat meer aandacht kan ontstaan voor het belang van een adequate interpretatie van DNA-gegevens.

- Er bestaat onduidelijkheid over de effectiviteit van grootschalig DNA-onderzoek voor het oplossen van misdrijven. Vanwege een grotere kans op 'mismatches' leidt een grotere DNA-databank niet zonder meer tot een hogere pakkans. Kan hiervoor een optimum worden gevonden?

[7] Hoewel de ministers politiek gezien een akkoord hebben bereikt, dient het formele besluit nog te worden genomen. Het oorspronkelijke voorstel is gepubliceerd onder nummer JAI(2007)3.
[8] Trb. 2005, 197

- Welke maatregelen kunnen worden getroffen voor een betere rechtsbescherming van burgers (naleving vernietigingsplicht, doelbinding, EU-uitwisseling van gegevens)?

Cameratoezicht

Het gebruik van toezichtcamera's in het publieke domein is in Nederland een betrekkelijk nieuw fenomeen. Rond 1999 begonnen lokaal de eerste experimenten en sindsdien is het gebruik van camera's in de openbare ruimte alleen maar toegenomen. Gemeenten zetten steeds vaker camera's in, met als doel de veiligheid te verbeteren en overlast te verminderen. Cameratoezicht op openbare plaatsen wordt vooral toegepast in uitgaans- en winkelcentra, op bedrijventerreinen en op en rond stations. Het grootste deel van de gemeenten ziet cameratoezicht als een aanvulling op andere maatregelen als surveillance en betere verlichting (Dekkers et al. 2007).

De Wet cameratoezicht op openbare plaatsen (2006)[9] reguleert het gebruik van camera's op openbare plaatsen. De gemeenteraad kan de burgemeester de bevoegdheid verlenen om, in het kader van de handhaving van de openbare orde, camera's te laten plaatsen. De burgemeester bepaalt de duur van de plaatsing en wijst de openbare plekken aan waar de camera's zullen worden geplaatst. Ook stelt hij de periode vast waarin de geregistreerde beelden rechtstreeks worden bekeken. Het cameratoezicht moet voor burgers kenbaar worden gemaakt, bijvoorbeeld door het aanbrengen van borden in het desbetreffende gebied. De camerabeelden vallen onder de Wet politieregisters en kunnen worden gebruikt voor de opsporing of vervolging van strafbare feiten (Vedder et al. 2007).

Cameratoezicht is toegestaan als andere middelen niet effectief blijken, de beslissing om camera's in te zetten in overeenstemming is met het doel van camera-inzet, het cameratoezicht aangekondigd is (heimelijk cameratoezicht is alleen onder strikte voorwaarden toegestaan) en de inbreuk op privacy van derden zo klein mogelijk is. Camerabeelden mogen maar voor een beperkte periode bewaard worden. Personen hebben recht op inzage in en verbetering, aanvulling, verwijdering en afscherming van persoonsgegevens.

Effecten cameratoezicht

Uit evaluatieonderzoek van Regioplan blijkt dat er over de effecten van cameratoezicht nog de nodige onduidelijkheid bestaat. De objectieve veiligheid (gemeten aan de hand van misdaadcijfers) blijkt na invoering van cameratoezicht in een aantal gemeenten toegenomen, maar in andere gemeenten afgenomen. Cameratoezicht lijkt uitgaansgeweld niet tegen te gaan, maar heeft mogelijk wel een positief effect op straatroof en (auto)inbraak en vergroot de pakkans na een incident (Dekkers et al. 2007). Ook over het effect op de subjectieve veiligheid, hoe veilig mensen zich voelen, bestaat discussie. Overheidsinformatie (2006) geeft aan dat cameratoezicht de subjectieve veiligheid duidelijk vergroot. De conclusie uit de meta-evaluatie van Regioplan is dat de subjectieve veiligheid na plaatsing van de camera's zowel kan toe- als afnemen.

[9] Stb. 2005, 392

Er is een aantal redenen te geven waarom de effecten van cameratoezicht niet duidelijk zijn. In de eerste plaats zijn de doelen van cameratoezicht vaak vrij algemeen geformuleerd ('vergroting van de veiligheid van burgers'; 'handhaving van en toezicht op de openbare orde') – wat deze doelen moeilijk meetbaar maakt. De effecten worden daarnaast gecompliceerd doordat cameratoezicht ertoe kan leiden dat er meer incidenten worden waargenomen en dat slachtoffers een grotere meldingsbereidheid hebben, als gevolg waarvan de geregistreerde misdaad toeneemt. Bovendien maakt cameratoezicht vaak deel uit van een pakket aan maatregelen, waardoor onduidelijk is in hoeverre de effecten daarvan aan het cameratoezicht kan worden toegeschreven (Dekkers et al. 2007).

Uit veel gemeentelijke evaluaties komt naar voren dat het live uitkijken van beelden een belangrijke voorwaarde is voor succesvol cameratoezicht. Op basis van signalen van de meldkamer kan de politie gerichter worden ingezet bij incidenten, wat een efficiënter gebruik van de politiecapaciteit mogelijk maakt. Ook kan de meldkamer inzoomen op situaties, wat identificatie van verdachten vergemakkelijkt. Het live uitkijken van beelden is wel een relatief dure maatregel (Dekkers et al. 2007).

Onder het publiek kan cameratoezicht op een groot draagvlak rekenen. Burgers lijken over het algemeen ook weinig moeite te hebben met de daarmee gepaard gaande inbreuk op hun privacy. Een aandachtspunt is hier wel dat burgers lang niet altijd weten dat ze worden gefilmd (Van Eijk et al. 2006; Dekkers et al. 2007). Beleidsonderzoeker Ger Homburg merkt hierover op dat de steun onder de bevolking minder groot zou kunnen zijn als mensen wisten op hoeveel plekken ze in de gaten worden gehouden (Binnenlands Bestuur 12 januari 2007).

Voor de situatie in Engeland, dat vooroploopt bij het gebruik van cameratoezicht, geldt een vergelijkbaar verhaal. De meeste Britse burgers zijn voorstander van bewakingscamera's. Tegelijkertijd kunnen daarbij kanttekeningen worden geplaatst. Ondanks het feit dat meer dan 100 camera's toezicht houden op Holloway Road in Londen, blijft de straat gevaarlijk: overvallen komen vaak voor en regelmatig wordt er ook een moord gepleegd. De organisatie Liberty stelt dat er geen bewijs is dat cameratoezicht in Engeland misdaad helpt voorkomen, maar dat cameratoezicht wel een groot deel van het beveiligingsbudget opslokt (NRC Handelsblad 14 juli 2007).

Filosoof Lynsey Dubbeld merkt op dat aan de privacywaarborgen rond cameratoezicht – de mogelijkheid tot inzage en correctie van beelden – lang niet altijd wordt voldaan (Dubbeld 2005). In een kwart van de gemeenten blijkt het niet mogelijk om als burger beelden terug te zien; in iets meer van een derde van de gemeenten bestaat er geen mogelijkheid voor correctie, het geven van een toelichting op de beelden. Daarbij moet worden aangetekend dat burgers in de praktijk ook niet of nauwelijks van die mogelijkheden gebruikmaken (Dekkers et al. 2007).

Recente ontwikkelingen

Een nieuwe ontwikkeling vormt het gebruik van intelligente camera's. Intelligente camera's kunnen niet alleen beelden registeren, maar deze beelden – en ook geluid – analyseren. Vervolgens kan bewakingspersoneel worden ingeseind als er iets bijzonders aan de hand is (NRC Handelsblad 4 april 2007). Dat maakt het mogelijk om op efficiënte wijze veel beelden tegelijk uit te kijken. Intelligente camera's kunnen met de volgende functies worden uitgerust: bewegingsdetectie, bewegingsanalyse, agressiedetectie en gezichtsherkenning (De Ingenieur 2005).

Er zijn nog wel problemen met de instelling van intelligente camera's. Zo hebben camera's moeite met het onderscheiden van twee onderdelen van een beeld, bijvoorbeeld een stilstaand persoon naast een stilstaande koffer. Proeven van de NS laten zien dat het opsporen van afwijkende gedragspatronen lastig is in een drukke en lawaaiige ruimte. Een te strakke instelling leidt tot vals positieve meldingen, terwijl een te losse instelling kan leiden tot het missen van incidenten. Een foutmarge van 1% levert in een druk station al een groot aantal fouten op. Ook gezichtsherkenning, zeker in menigten, is nog niet goed mogelijk.

Nationaal Coördinator Terrorismebestrijding Joustra heeft de verwachting uitgesproken dat camera's ingezet kunnen worden voor terrorismebestrijding. Met behulp van slimme camera's zouden patronen van afwijkend gedrag kunnen worden herkend (NRC Handelsblad 4 maart 2006). Gezien de huidige problemen met gedrags- en gezichtsherkenning lijkt dat voorlopig echter niet tot de mogelijkheden te behoren.

Een tweede ontwikkeling betreft een dusdanige uitbreiding van cameratoezicht dat personen voortdurend gevolgd kunnen worden in bijvoorbeeld het centrum van een grote stad. Zeker als camera's onderdeel gaan uitmaken van een netwerk aan sensoren, komen dergelijke toepassingen binnen handbereik. Zo zouden camerabeelden gekoppeld kunnen worden aan locatiegegevens van mobiele telefoons. Ook kunnen camerabeelden met nummerplaatherkenning worden gekoppeld aan politieregisters of databestanden met niet-betaalde boetes of openstaande belastingschulden. Een dergelijke ontwikkeling past goed in de visie van een 'nodale oriëntatie' binnen de opsporing, waarbij grote infrastructurele knooppunten stelselmatig in de gaten worden gehouden (zie de passage over informatiegestuurde opsporing).

Tot op heden zijn publiek en privaat cameratoezicht gescheiden regimes. Het is echter de vraag of deze scheiding op den duur gehandhaafd blijft. Camerabeelden afkomstig uit het private domein kunnen nu al door opsporingsdiensten worden opgevraagd. Ook komt het voor dat in gemeentelijke of regionale uitkijkruimtes zowel publieke als private beelden worden bekeken. De stap naar koppeling van beide soorten beelden lijkt dan niet meer zo ver weg – en zou ook passen binnen een 'nodale oriëntatie'.

Aandachtspunten cameratoezicht

Cameratoezicht wordt meer en meer een alledaagse technologie. Steeds meer gemeenten gaan er toe over om ze te plaatsen. Bij deze ontwikkeling kunnen evenwel diverse kanttekeningen worden geplaatst:

- Evaluatieonderzoek van cameratoezicht geeft een wisselend beeld van het effect op de objectieve en subjectieve veiligheid. Daar zijn moeilijk conclusies uit te trekken. Er is dan ook behoefte aan meer onderzoek naar de effectiviteit van cameratoezicht.

- Er is meer duidelijkheid nodig over de doelstellingen van cameratoezicht. Deze zijn vaak vaag geformuleerd, wat de discussie over nut en noodzaak ervan vertroebelt. Moet cameratoezicht vooral dienen om kleine criminaliteit terug te dringen, moet het de pakkans na misdrijven vergroten of kan het ook behulpzaam zijn bij het voorkomen van terreuraanslagen?

- Burgers zijn niet altijd op de hoogte van cameratoezicht. Ook lijkt meer aandacht nodig voor de privacywaarborgen rond cameratoezicht – het recht op inzage en correctie van beelden.

Tot slot

Als we de verschillende casusposities overzien, kunnen de volgende, terugkerende aandachtspunten worden vastgesteld:

- Over de effectiviteit van de besproken veiligheidsmaatregelen (gebruik van databanken, DNA-onderzoek, cameratoezicht) bestaan weinig cijfers. De effectiviteit kan vaak moeilijk worden aangetoond – maar ook moeilijk weerlegd. De vraag naar de effectiviteit van maatregelen wordt vaak gesteld vanuit privacyperspectief, vanwege de (mogelijke) inbreuken op de privacy die ermee gepaard gaan. Deze vraag is echter minstens zo relevant vanuit opsporingsperspectief. Onze veiligheid is immers niet gediend met ineffectieve methoden.

- De betrouwbaarheid van gegevens en een adequate interpretatie daarvan zijn van groot belang. Vervuilde bestanden en foutmarges kunnen leiden tot een groot aantal vals positieve uitkomsten. Zowel vanuit het gezichtspunt van de rechtsbescherming van burgers als vanuit het opsporingsperspectief vormt dat een probleem.

- De rechtsbescherming van burgers vormt een belangrijk aandachtspunt: welke mogelijkheden hebben burgers om in beroep te gaan tegen een onterechte signalering of verdachtmaking?

- De belangrijkste trend – zowel nationaal als internationaal – betreft het koppelen en analyseren van databestanden (al dan niet in combinatie met DNA-banken of camerabeelden) voor preventief onderzoek naar potentieel verdacht gedrag. Het is de vraag of het instrument van datamining hiervoor ver genoeg ontwikkeld is. Valt er meer te verwachten van een gerichte inzet van maatregelen (*select before you collect*)? Hiermee verband houdend is het de vraag of niet meer helderheid nodig is over de specifieke doelen die beoogd worden met veiligheidsmaatregelen.

- De wettelijke bevoegdheden voor opslag, gebruik, uitwisseling en bescherming van persoonsgegevens zijn divers en nogal eens op weinig samenhangende wijze geregeld. Dat maakt het lastig om verantwoorde keuzes te maken bij de evaluatie van deze wettelijke bepalingen. Het is de vraag hoe daarin kan worden voorzien.

Literatuur

Binnenlands Bestuur (2007). Cameratoezicht: veiligheid én schijnveiligheid. 12 januari 2007.

Boersma, J. (2007). Need for nodes. (http://www.spl.politieacademie.nl/files/sll3%20need%20for%20nodes.doc)

Broeders, A.P.A. (2006). Of earprints, fingerprints, scent dogs, cot deaths and cognitive contamination – a brief look at the present state of play in the forensic arena. In: Forensic Science International 159: 148-157.

Broeders, A.P.A. (2005). Ontwikkelingen in de criminalistiek. Van vingerspoor tot DNA-profiel – van zekerheid naar waarschijnlijkheid. Den Haag: Boom Juridische Uitgevers.

Buiter, L., M.J. Dubelaar, N.C.W. Haesen, R. Malewicz, J.F. Nijboer, Th.A. de Roos & L.G. Toornvliet (2003). DNA-onderzoek in opsporing en bewijsvoering in strafzaken. DNA- nulmeting. Leiden: Universiteit van Leiden (rapport WODC).

Commissie-Bosma (Adviescommissie informatiestromen Veiligheid) (2007). Data voor daadkracht. Gegevensbestanden voor veiligheid, observatie en analyse. Den Haag.

De Ingenieur (2005). Digitale slotgracht, automatische gezichtsherkenning is nog niet mogelijk. 12 augustus 2005.

Dekkers, S. & G. Homburg (2006). Evaluatie cameratoezicht op openbare plaatsen. Nulmeting. Amsterdam: Regioplan.

Dubbeld, L. (2005). Protecting personal data in camera surveillance practices. In: Surveillance & society, 2(4): 546-563. (www.surveillance-and-society.org)

Eijk, A. van, G. Kanning, A. Molenaar, M. Strijbos & W. Bernasco (2006). Publiek niet op de hoogte van aanwezigheid camera's. (http://www.kennislink.nl)

GOVCERT (2007). Trendrapport 2007. Cybercrime in trends en cijfers. Den Haag: GOVCERT.NL.

Jacobs, B. & M. Jochems (2007). DigiD & privacy. Aanvraag- en activeringsprocedures zijn te zwak. In: Automatiseringsgids 19 oktober 2007.

Koops, B.J. (2006). Tendensen in opsporing en technologie. Nijmegen: Wolf Legal Publishers.

Kruisbergen, E.W. en C.J. de Poot (2007). Toepassing van DNA-wetgeving in de praktijk: nog veel onbeantwoorde vragen. In: Nederlands juristenblad, 82 (28): 1728-1735.

Ministerie van Justitie (2007). Meer DNA-onderzoek bij de aanpak van criminaliteit. Persbericht ministerie van Justitie 11 juli 2007.

Muller, E.R., H.R.B.M. Kummeling & R.P. Bron (2007). Veiligheid en privacy. Een zoektocht naar een nieuwe balans. Den Haag: Boom Juridische Uitgevers.

Neve, R., L. Vervoorn, F. Leeuw & S. Bogaerts (2006). Eerste inventarisatie van contraterrorismebeleid: Duitsland, Frankrijk, Italië, Spanje en de Verenigde Staten – 'research in progress'. Den Haag: WODC.

Overheidsinformatie (2006). Effect van groeiend cameratoezicht onduidelijk. 22 augustus 2006.

Raad van Hoofdcommissarissen (2004). Spelverdeler in de opsporing. Een visie op forensische opsporing. (http://www.politie.nl/ImagesLandelijk/spelverdeler%20in%20opsporing_tcm31-144778.pdf)

Rathenau Instituut (2007). RFID: Helderheid over opsporing verzocht. Bericht aan het parlement. Den Haag: Rathenau Instituut.

Vedder, A., L. van der Wees, B.J. Koops & P. de Hert (2007). Van privacyparadijs tot controlestaat? Misdaad- en terreurbestrijding in Nederland aan het begin van de 21ste eeuw. Den Haag: Rathenau Instituut.

Wetgevingsoverzicht

Overzicht van aanhangige en aangekondigde wetgeving waarin gegevensbescherming een belangrijke rol speelt.[10]

Nationale wetgeving

Ratificatie PNR-Verdragen tussen de EU en de VS respectievelijk de EU en Australië (goedkeuringswetten in voorbereiding).
Regelt de verplichte overdracht van Passenger Name Records aan de Amerikaanse respectievelijk Australische autoriteiten bij vluchten vanuit de EU naar de VS respectievelijk Australië.

Wetvoorstel invoering kilometerbeprijzing (in voorbereiding).
Regelt onder meer de modaliteiten voor de kilometerheffing.

Wetsvoorstel Elektronisch Kinddossier (in voorbereiding).
Regelt onder meer de landelijke eisen voor standaarden voor het elektronisch kinddossier. De digitaliseringsplicht is reeds opgenomen in het wetsvoorstel Publieke Gezondheid (Kamerstukken 31316).

Wet Elektronisch Patiëntendossier (wijziging Wet Burgerservicenummer in de zorg).
Regelt de randvoorwaarden voor een veilige en zorgvuldige invoering van een landelijk elektronische patiëntendossier (EPD), waardoor bepaalde medische gegevens van een patiënt altijd actueel en beschikbaar zijn en maar één keer hoeven te worden ingevoerd.

Wijziging van de Paspoortwet in verband met het herinrichten van de reisdocumentenadministratie (in behandeling TK, Kamerstukken 31324).
Regelt onder meer toegang van de rechtshandhavingsdiensten tot de databank met vingerafdrukken die in paspoorten zijn opgenomen.

Wet verplichte medewerking aan een bloedtest in strafzaken (in behandeling EK, Kamerstukken 31241).
Dit wetsvoorstel maakt het mogelijk dat een verdachte of een derde wordt verplicht mee te werken aan onderzoek, aan de hand waarvan kan worden vastgesteld of hij drager is van een virus dat bij het plegen van een strafbaar feit kan zijn overgedragen op het slachtoffer.

[10] Dit overzicht van wetgeving is mogelijk niet uitputtend. Wel is naar volledigheid gestreefd.

Wet bewaarplicht telecommunicatiegegevens (in behandeling EK, Kamerstukken 31145).
Regelt verplichte opslag van alle telefoon-, fax-, e-mail- en internetgegevens door de providers voor een duur van 12 maanden.

Wijziging van de Wet op de Inlichtingen- en Veiligheidsdiensten (in behandeling EK, Kamerstukken 30553).
Regelt onder meer de beschikbaarstelling van geautomatiseerde gegevensbestanden door de desbetreffende bestuursorganen en aangewezen instanties ten behoeve van data-analyse en het bevorderen of treffen van maatregelen ter bescherming van door een dienst te behartigen belangen.

Wet implementatie EG-richtlijnen energie-efficiëntie (in behandeling EK, Kamerstukken 31320).
Bevat een verplichting voor energieleveranciers om zogenoemde 'slimme meters' bij hun klanten te plaatsen. Deze meters kunnen op afstand worden uitgelezen en bieden bovendien de mogelijkheid het energieverbruik van de eindgebruikers te beïnvloeden.

Uitbreiding bestuurlijke handhaving volksgezondheidswetgeving (in behandeling EK, Kamerstukken 31122).
Geeft de Inspectie voor de Gezondheidszorg de bevoegdheid om patiëntendossiers in te zien, ook zonder toestemming van de betrokkene.

Verplichte medewerking aan een bloedtest in strafzaken (in behandeling EK, Kamerstukken 31241).
Dit wetsvoorstel maakt het mogelijk dat een verdachte of een derde wordt verplicht mee te werken aan onderzoek, aan de hand waarvan kan worden vastgesteld of hij drager is van een virus dat bij het plegen van een strafbaar feit kan zijn overgedragen op het slachtoffer.

Verwijsindex risicojongeren (in voorbereiding; verschijnt naar verwachting begin 2009).
Regelt de blinde koppeling van de bestanden van jongerenwerkers uit verschillende disciplines. Er worden geen gegevens in één dossier geplaatst, maar wel signaleringen verspreid wanneer met betrekking tot een bepaalde jongere nieuwe informatie wordt opgevoerd.

Europese regelgeving

Verordening betreffende het Visum Informatiesysteem (VIS) en de uitwisseling tussen de lidstaten van informatie op het gebied van visa voor kort verblijf (ingediend, COM(2004)835).
Het VIS bevat informatie over alle personen die een visum voor de EU aanvragen, ongeacht of de aanvraag is geaccepteerd of afgewezen. In een nieuwe versie van het VIS worden ook biometrische gegevens opgeslagen.

Verordening en besluit betreffende het Schengen Informatiesysteem (SIS) van de tweede generatie (ingediend, COM(2005)236 en COM(2005)230).
Het SIS wordt gebruikt ter ondersteuning van de bewaking van de buitengrenzen van het Schengengebied en ter bevordering van het vrije verkeer van personen binnen het gebied. In de nieuwe versie, SIS II, die eind 2008 in gebruik moet worden genomen, zullen tevens biometrische kenmerken en foto's worden opgenomen. Naast de douane hebben ook politie en justitie toegang tot het SIS.

Besluit betreffende de oprichting van de Europese Politiedienst (Europol) (ingediend, COM(2006)817).
Regelt onder meer de geautomatiseerde verwerking door Europol van opsporingsinformatie.

Kaderbesluit bescherming van persoonsgegevens die worden verwerkt in het kader van politiële en justitiële samenwerking (ingediend, COM(2005)475).
Regelt onder meer de voorwaarden waaronder gegevens mogen worden uitgewisseld tussen lidstaten van de EU.

Kaderbesluit over het gebruik van persoonsgegevens van passagiers (PNR-gegevens) voor wethandhavingsdoeleinden (ingediend, COM(2007)654).
Regelt het opzetten van een systeem om ook in de EU passagiersgegevens te verzamelen.

Kaderbesluit betreffende de organisatie en de inhoud van uitwisselingen van gegevens uit het strafregister tussen de lidstaten (ingediend, COM(2005)690).
Ziet toe op de organisatie en inhoud van uitwisselingen van gegevens uit het strafregister tussen de lidstaten. Op termijn dienen deze uitwisselingen volledig geautomatiseerd te verlopen.

Verordening tot wijziging van de gemeenschappelijke visuminstructies in verband met de invoering van biometrische identificatiemiddelen (ingediend, COM(2006)269).
Maakt het mogelijk biometrische gegevens (vingerafdrukken, digitale foto) af te nemen bij personen die een EU-visum willen aanvragen.

Wetgevend voorstel om biometrische gegevens van EU-burgers en derdelanders op te slaan (verschijnt naar verwachting medio 2009).
Beoogt het in- en uitreizen van de Europese Unie te vereenvoudigen voor bona fide reizigers uit derde landen en EU-burgers.

Nieuw meerjarenkader voor het beleid op het terrein van Justitie en Binnenlandse Zaken (verschijnt naar verwachting eind 2009).
Zal naar verwachting onder meer de uitwerking bevatten van de clausules uit het Verdrag van Lissabon die zijn gericht op gegevensbescherming. Mogelijk worden ook andere wetgevende voorstellen aangekondigd waarbij gegevensbescherming een rol speelt.

Discussiestellingen

Gebruik van databanken:

- De risico's van incorrecte data en identiteitsfraude zijn te groot voor een verantwoord gebruik van databanken en gegevensuitwisseling.
- Politie en AIVD moeten kunnen dataminen om potentieel crimineel gedrag en voorbereidende terroristische handelingen op te sporen.
- De rechtsbescherming van burgers is met de huidige wetgeving voldoende gewaarborgd.

DNA-onderzoek:

- Opsporingsambtenaren en rechters hechten te veel waarde aan de bewijskracht van DNA-data.
- De opslag van DNA-profielen en de uitwisseling daarvan met andere landen moeten niet alleen ten dienste staan van de opsporing van zware vergrijpen, maar ook van lichtere misdrijven als woninginbraak en winkeldiefstal.

Cameratoezicht:

- Cameratoezicht dient zowel kleine criminaliteit te voorkomen als nieuwe terreuraanslagen.
- Nut en noodzaak van cameratoezicht zijn meer een geloofsartikel dan een aangetoond feit.