Rathenau Instituut

Bericht aan het Parlement

OKTOBER 2008

Opsporing behoeft 'checks and balances'

Nieuwe technologieën als datamining, DNA-onderzoek en (grootschalig) camera-toezicht moeten politie en justitie ondersteunen in de strijd tegen misdaad en terreur. De verwachtingen daarvan zijn hooggespannen. In dit Bericht aan het Parlement maakt het Rathenau Instituut duidelijk dat deze opsporingsmethoden niet de wondermiddelen zijn waarvoor ze vaak worden aangezien. Aan de inzet ervan kleven risico's. Deze risico's ondermijnen de effectiviteit van veiligheidsmaatregelen en kunnen ingrijpende gevolgen hebben voor burgers. Optimaal gebruik van hightech opsporingsmethoden vereist dan ook een betere afweging tussen doel en middel. Dat vergt meer inzicht van de politiek in de schaal waarop en de situaties waarin opsporings- en veiligheidsdiensten gebruikmaken van hun bevoegdheden. Ook moeten burgers meer mogelijkheden krijgen zich te verweren tegen onterechte verdachtmakingen.

Het Rathenau Instituut adviseert het parlement:

1 Verbeter het toezicht op opsporings- en veiligheidsdiensten.

2 Zet de architectuur van datasystemen op de politieke agenda.

3 Kijk kritisch naar de beroepsmogelijkheden voor burgers.

Achtergrondinformatie

Project Screening Society

Met dit Bericht aan het Parlement rondt het Rathenau Instituut het project Screening Society af. In Screening Society zetten we de gevolgen van de groeiende lijst veiligheidsmaatregelen voor onze privacy en rechtsbescherming, op een rij. Dit resulteerde in 2007 in de publicatie 'Van privacyparadijs tot controlestaat?'. Op 20 maart 2008 organiseerde het Rathenau Instituut samen met de commissie voor Justitie van de Eerste Kamer een expertbijeenkomst over gegevensbescherming. Het verslag van deze bijeenkomst is verschenen als Kamerstuk (I 2007/8 – 31200 VI, F).

De resultaten van de publicatie en de expertmeeting zijn in dit Bericht aan het Parlement verwerkt. Ook in het nieuwe werkprogramma (2009 - 2010) blijft het Rathenau Instituut aandacht besteden aan het thema veiligheid.

Hightech opsporing

Binnen het opsporingsapparaat bestaan hoge verwachtingen van de inzet van technologie. DNA-onderzoek, cameratoezicht, het aftappen van (mobiele) telefonie en internet, computeronderzoek en het koppelen en analyseren van databestanden moeten de strijd tegen criminelen en terroristen gemakkelijker maken. Zo moet het forensisch gebruik van DNA-profielen het oplossingspercentage van misdrijven fors opschroeven en kunnen camerabeelden de bewijsvoering in de rechtszaal ondersteunen. Veel politiële en justitiële bevoegdheidsverruimingen van de afgelopen jaren zijn toegesneden op nieuwe technologie.

Digitale veiligheid

De belangrijkste ontwikkeling is het koppelen en analyseren van digitale databestanden. Met computerprogramma's kunnen gegevens uit allerlei bronnen met elkaar worden gecombineerd en geanalyseerd (datamining). Zo kunnen bijvoorbeeld de gegevens uit de databestanden van de sociale dienst, de Kamer van Koophandel of de Albert Heijn-bonuskaart met elkaar worden vergeleken.

Politie en justitie kunnen zo in een vroeg stadium (potentieel) criminele of terroristische activiteiten op het spoor komen. Criminele en terroristische groepen maken steeds vaker gebruik van moderne communicatiemiddelen. Politie en justitie kunnen hierbij moeilijk achterblijven. Alleen zo vinden opsporings- en veiligheidsdiensten aansluiting bij de moderne netwerksamenleving. Deze speelt zich allang niet meer alleen in de 'reële' wereld af, maar ook in de virtuele. De door de Europese Unie verplichte opslag van verkeersgegevens door telecommunicatiebedrijven moet in dit licht worden bezien. Door het traceren van het bel- en e-mailverkeer en het surfgedrag op internet kunnen verdachte netwerken in kaart worden gebracht.

Het gebruik van digitale databestanden leidt ook bij andere maatregelen tot nieuwe of uitgebreidere vormen van toezicht en controle. Zo kunnen 'slimme' camera's worden uitgerust met nummerplaatherkenning en gekoppeld worden aan politieregisters. Of kunnen gegevens van DNA-databanken worden uitgewisseld met andere EU-lidstaten.


SECURITY CHECK
ALL COMMENTS REGARDING WEAPONS, DANGEROUS OBJECTS OR HIJACKING ARE TAKEN SERIOUSLY
PLEASE, NO JOKES

Kanttekeningen

Bij het gebruik van moderne technologie voor opsporings- en veiligheidsdoeleinden kunnen kanttekeningen worden geplaatst. Dragen methoden als datamining en cameratoezicht daadwerkelijk bij aan een betere bestrijding van misdaad en terreur? Hoe betrouwbaar zijn ze? Met welke risico's gaan ze gepaard? Deze vragen zijn niet alleen van belang vanwege de privacy of rechtsbescherming van de burger. Ze zijn minstens zo relevant vanuit opsporingsperspectief. Opsporing en veiligheid zijn niet gebaat bij ineffectieve methoden.

Effectiviteit

Onderzoek naar de effectiviteit van veiligheidsmaatregelen levert vooral nieuwe vragen op. Zo kampt datamining met problemen als bestandsvervuiling en een overvloed aan informatie. Verdient een meer gerichte inzet ('select before you collect') niet de voorkeur? Deze vraag heeft ook gevolgen voor de inrichting van datasystemen: dienen ze gericht te zijn op een maximale vergaring van informatie of moeten we juist streven naar dataminimalisatie?

Onheldere doelstelling

Veiligheidsmaatregelen worden vaak gelegitimeerd met de strijd tegen zware misdaad en terreur. Maar, maatregelen als DNA-onderzoek of cameratoezicht blijken vooral behulpzaam voor het oppakken van plegers van volumecriminaliteit als straatroof of woninginbraak. Dat roept de vraag op waarvoor de maatregelen nu eigenlijk zijn bedoeld. Vangen we hiermee wie we moeten vangen? Deze discussie lijkt niet of nauwelijks te worden gevoerd.

Rechtsbescherming

Door de inzet van hightech opsporingsmethoden worden burgers sneller dan voorheen onderwerp van politieel of justitieel onderzoek. Vaak zonder dat ze daar zelf weet van hebben. Incorrecte data, identiteitsdiefstal of een toevallige samenloop van omstandigheden kunnen ertoe leiden dat personen ten onrechte als (potentieel) crimineel of terrorist worden aangemerkt. Vaak heeft dit ingrijpende gevolgen voor het leven van de betrokkenen: geblokkeerde bankrekeningen, reisbeperkingen, hinderlijke controle ('verstoring') door de politie. Zolang de kwestie niet tot een rechtszaak leidt, lijken burgers weinig beroepsmogelijkheden te hebben. Hoe verkrijg je inzage in je AIVD-dossier? Hoe kun je verweer aantekenen tegen een onterechte beschuldiging door de politie? Dat roept de vraag op of de rechtsbescherming van burgers geen versterking behoeft.

Inzicht ontbreekt

De politiek mist zicht op de schaal waarop politie en justitie gebruikmaken van hun bevoegdheden, in wat voor situaties ze dat doen en hoe groot de risico's zijn van onterechte verdenkingen. Dit, opgeteld bij onduidelijke doelstellingen en effecten van maatregelen, maakt het onmogelijk om politieke uitspraken te doen over een 'proportionele inzet' van veiligheidsmaatregelen. Vanwege het risico van onterechte verdachtmaking, vormt dat een probleem. Dat geldt zowel op nationaal als Europees niveau. Er is dan ook dringend behoefte aan meer politiek inzicht in, en toezicht op de praktijk van opsporings- en veiligheidsdiensten. De uitkomsten van de expertbijeenkomst van 20 maart 2008 (zie pagina 2) onderstrepen deze conclusie.

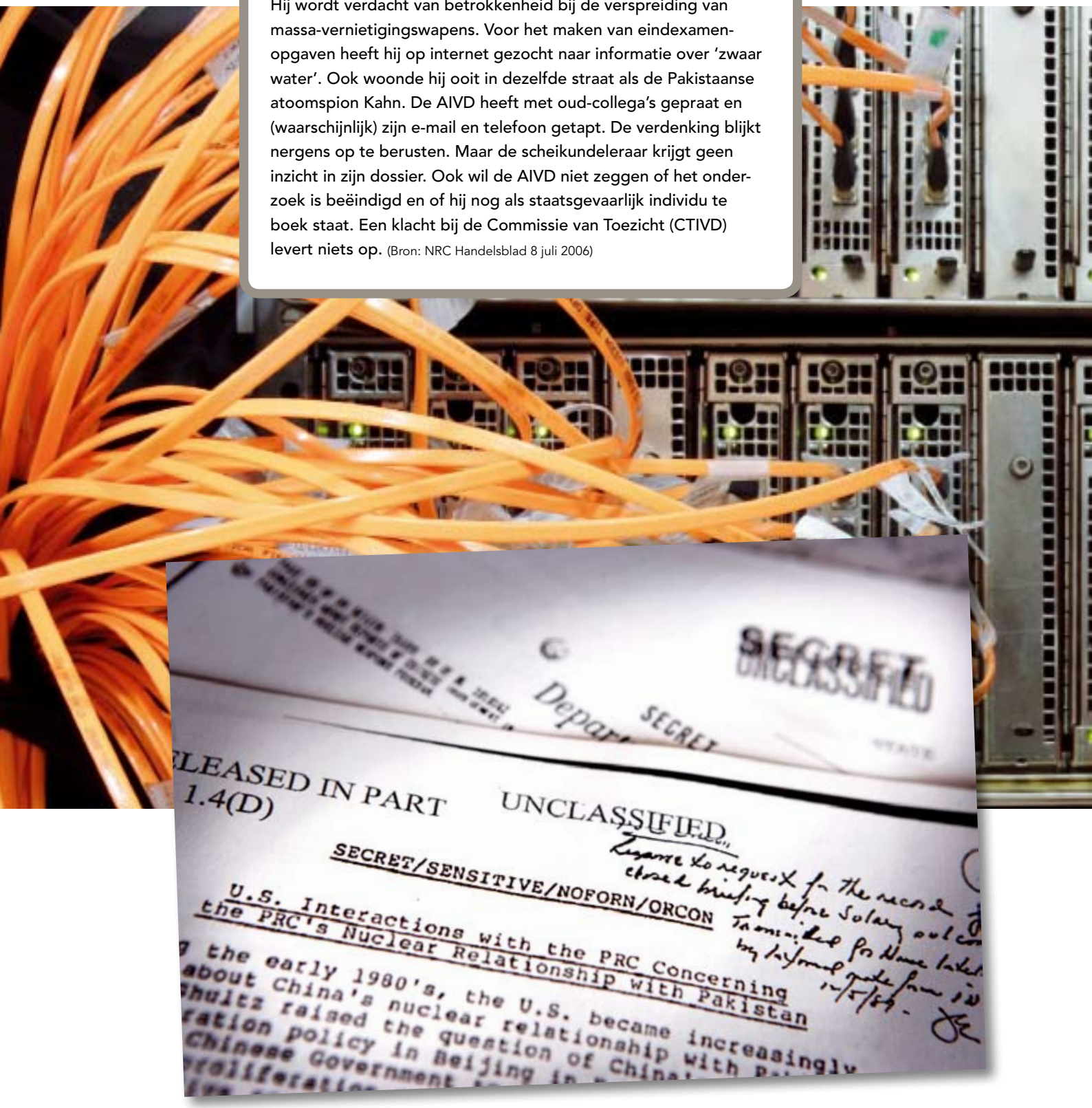
Drie trends

Op de volgende pagina's gaan we aan de hand van drie trends nader in op het gebruik van moderne opsporingsmethoden: datamining, een brede inzet van veiligheidsmaatregelen en internationale gegevensuitwisseling.

Trend 1:

Staatsgevaarlijk

Een voormalig scheikundeleraar krijgt bezoek van de AIVD. Hij wordt verdacht van betrokkenheid bij de verspreiding van massa-vernietigingswapens. Voor het maken van eindexamen-opgaven heeft hij op internet gezocht naar informatie over 'zwaar water'. Ook woonde hij ooit in dezelfde straat als de Pakistaanse atoomspion Kahn. De AIVD heeft met oud-collega's gepraat en (waarschijnlijk) zijn e-mail en telefoon getapt. De verdenking blijkt nergens op te berusten. Maar de scheikundeleraar krijgt geen inzicht in zijn dossier. Ook wil de AIVD niet zeggen of het onderzoek is beëindigd en of hij nog als staatsgevaarlijk individu te boek staat. Een klacht bij de Commissie van Toezicht (CTIVD) levert niets op. (Bron: NRC Handelsblad 8 juli 2006)



Datamining

Digitale voetsporen

In ons dagelijks leven laten we voortdurend digitale voetsporen achter: als we (mobiel) bellen, op internet surfen, geld pinnen, met de OV-chipkaart reizen of met een klantenkaart boodschappen doen. Al deze gegevens worden opgeslagen in databestanden. Opsporings- en veiligheidsdiensten zijn wettelijk bevoegd deze gegevens op te vragen. De handel en wandel van personen kan tot in detail worden nagegaan. De burger is daarmee transparant geworden voor het opsporingsapparaat.

Risicoprofielen

Een belangrijke trend betreft het koppelen en analyseren van databestanden (datamining). Met behulp van risicoprofielen kunnen bestanden worden doorzocht op patronen van 'afwijkend' of 'potentieel verdacht' gedrag. Zo kunnen criminele of terroristische activiteiten in een vroeg stadium worden opgespoord. Maar deze gedigitaliseerde informatievergaring brengt ook risico's met zich mee: datamining vereist dat de beschikbare data betrouwbaar zijn en dat ze adequaat worden geïnterpreteerd.

Vals positief

Aan deze voorwaarden wordt lang niet altijd voldaan. Bestandsvervuiling, bijvoorbeeld door spelfouten, vormt een groot probleem. Zo bleek op een gegeven moment met vijf procent van alle Sofinummers iets mis te zijn. Wat betekent dat voor de opvolger van het sofinummer, het Burgerservicenummer? Identiteitsdiefstal vormt ook een groeiend probleem: een slimme crimineel 'leent' andermans identiteit voor hij zijn slag slaat.

Daarnaast is het lastig om computerdata, die vaak van hun context zijn ontdaan, goed te interpreteren. Door een toevallige combinatie van factoren kan iemand plotseling tot een risicogroep horen: zie het voorbeeld van de scheikundeleraar. Als gevolg van bestandsvervuiling, identiteitsdiefstal of misinterpretatie worden mensen ten onrechte als mogelijk crimineel of staatsgevaarlijk individu bestempeld.

Informatiehonger

Hoe groter de (gekoppelde) databestanden zijn en hoe langer de bewaartermijn van gegevens is, hoe groter de kans op incorrecte data en identiteitsdiefstal. De bestaande neiging van het opsporingsapparaat om zoveel mogelijk data te vergaren – onder het mom 'je weet nooit waar het goed voor is' – moet daarom kritisch worden bezien. Deze informatiehonger kan tot onwerkbare hoeveelheden informatie leiden, die de opsporing niet ten goede komen.

Trend 2: Brede inzet

Mobiel banditisme

Geen automobilist passeert nog ongemerkt het snelweg-knooppunt van de A28 en de A50 bij Zwolle. De politie IJsselland registreert met camera's alle voertuigen en vergelijkt de beelden met opgeslagen kentekens in politie-bestanden. Met als doel opsporing van 'mobiel banditisme'. De camerabeelden kunnen ook worden gekoppeld aan bestanden met openstaande boetes of belastingschulden. Deze ontwikkeling past binnen een 'nodale oriëntatie', waarbij de politie stelselmatig grote infrastructurele knooppunten in de gaten houdt. (Bron: NRC Handelsblad 14 mei 2008)

De alomtegenwoordige camera

In de centra van de grote steden observeren honderden camera's het winkelende en uitgaande publiek. In de regio Den Haag hangen er inmiddels meer dan vierhonderd. Als de camera's in het openbaar vervoer en op het Binnenhof worden meegeteld, zijn dat er zelfs duizend: cameratoezicht in het publieke domein heeft een hoge vlucht genomen.

Maar uit evaluatieonderzoek blijkt dat cameratoezicht lang niet altijd het effect heeft waarvoor het bedoeld is. Zo lijkt cameratoezicht uitgaansgeweld niet tegen te gaan. Het heeft mogelijk wel effect op straatroof en (auto)inbraak en het vergroot de pakkans na een incident. Maar het is de vraag of dit laatste voldoende grond is voor de uitbreidingsplannen van veel gemeenten. Discussie over de precieze doelstellingen van cameratoezicht vindt nauwelijks plaats.

Nieuwe, 'slimme' toepassingen als automatische kentekenregistratie zijn een volgende stap in het gebruik van camera's. Ook hierover vindt weinig discussie plaats. Dienen deze middelen te worden ingezet om criminelen en terreurgroepen te traceren, of om achterstallige parkeerboetes en belastingschulden te innen? Het eerste motief lijkt soms niet meer dan een excuus voor het laatste.

veiligheidsmaatregelen

Mag ik uw wangslijm?

Ook andere veiligheidsmaatregelen worden steeds breder ingezet. De wettelijke drempel voor afname van DNA-materiaal is de afgelopen jaren verlaagd naar misdrijven met een maximumstraf van vier jaar. Daaronder vallen woninginbraak en winkeldiefstal. Een uitbreiding naar DNA-afname bij stelselmatige daders van eenvoudige delicten als vernieling is in de maak. Het aantal opgeslagen profielen in de nationale databank is hierdoor sterk gegroeid, tot inmiddels meer dan 60.000. De profielen worden twintig tot dertig jaar bewaard.

Het nut van DNA-onderzoek is echter niet onomstreden. De weinige cijfers die daarover bestaan, tonen aan dat het slechts tot een geringe stijging van het oplossingspercentage van misdrijven leidt. Met de groei van de databank en de lengte van de bewaartermijn neemt bovendien het risico op 'mismatches' toe. Dit risico wordt nog eens extra vergroot door de slechte naleving van de wettelijke plicht om materiaal van niet-veroordeelden te vernietigen.

Ook voor DNA-onderzoek geldt dus de vraag hoe het doel ervan zich verhoudt tot het middel en de daarmee gepaard gaande risico's. De internationale uitwisseling van DNA-gegevens volgens het Verdrag van Prüm beoogt grensoverschrijdende criminaliteit te bestrijden. Is dat doel gediend met een jarenlange opslag van gegevens van – bijvoorbeeld – jongeren die zijn opgepakt voor een relatief licht vergrijp als winkeldiefstal?

Trend 3: Internationale gegevensuitwisseling

Vast in eigen land

Tegen een Nederlandse zakenman loopt een Europees arrestatiebevel. Zijn mobiele nummer wordt in verband gebracht met een Griekse fraudezaak. De verdenking berust op een foutieve gegevenskoppeling: tijdens de fraude was het mobiele nummer niet van hem. Wegens het risico van arrestatie aan de grens kan hij een jaar lang niet op reis. Mogelijkheden om in beroep te gaan ontbreken. Verzoeken van het ministerie van Justitie tot opheffing van het arrestatiebevel worden in Griekenland genegeerd. Het bevel wordt pas ingetrokken nadat enkele Europarlementariërs aan de bel trekken. (Bron: NRC Handelsblad 3 januari 2008; Rondom Tien 24 mei 2008)

Europees netwerk

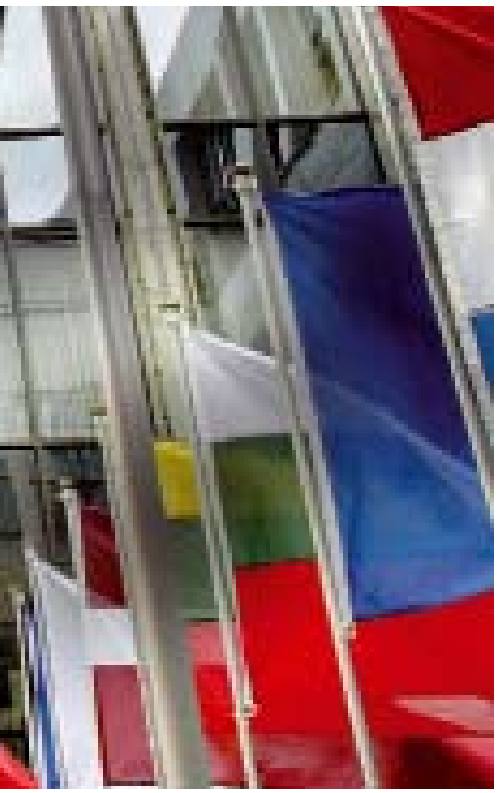
De lidstaten van de Europese Unie werken steeds intensiever samen in hun streven criminaliteit te bestrijden en terreuraanslagen te voorkomen. Deze samenwerking krijgt gestalte in de uitwisseling van gegevens uit nationale databestanden, zoals politieregisters of DNA-databanken. Daarnaast worden Europabrede datasystemen opgezet. Het gaat hierbij al snel om grote hoeveelheden informatie. Zo bevat het Schengen Informatie Systeem (SIS), dat de buitengrenzen van het Schengengebied bewaakt, de gegevens van honderdduizenden personen. En het Visum Informatie-systeem (VIS), dat biometrische informatie (foto's en vingerafdrukken) opslaat van iedereen die een Europees visum aanvraagt, kan de gegevens van maar liefst 70 miljoen personen bevatten.

Knelpunten

Het Europese informatienetwerk roept dezelfde vragen op als die bij datamining. Zo valt de betrouwbaarheid van de gegevens in het Schengen Informatie Systeem lastig te verifiëren. Diverse instanties kunnen data invoeren en de criteria daarvoor verschillen per land. Ook blijkt uit onderzoek van dataprotectie-autoriteiten dat een aanzienlijk deel van de registraties op een onjuiste rechtsgrondslag berust.

En hoe zit het met de effectiviteit van de informatiesystemen? Voor de opvolger van het Schengen Informatie Systeem, het nog in te voeren SIS II, heeft de Europese Commissie voorstellen gedaan voor elektronische grensbewaking met behulp van biometrische gegevens. Mensen met een Europees paspoort of een legale verblijfstitel kunnen de grens daardoor gemakkelijker passeren, zonder persoonlijke controle door politie of douane. Maar een 'impact assessment' van de plannen voor SIS II wijst uit dat deze negatief uitpakken voor het doel van terrorismebestrijding. Eerdere aanslagplegers in Europa zouden er niet door zijn tegengehouden, omdat zij over zo'n paspoort of verblijfstitel beschikten.

Daarnaast ontbreekt een uniform stelsel voor gegevensbescherming. Zo hekelt Europees privacytoezicht-



houder Peter Hustinx de recente uitbreiding door de EU-ministers van Justitie van het Verdrag van Prüm. Dit verdrag regelt de uitwisseling van gegevens uit nationale DNA-databanken. De 27 lidstaten hebben verschillende wetten en regels voor gegevensbescherming. Dat maakt het voor burgers moeilijk bezwaar aan te tekenen als ze ten onrechte ergens van worden verdacht.

Parlementaire controle

Een bijkomend probleem is dat de nationale parlementen weinig zicht hebben op de Europese regelgeving. Ook lijken nationale parlementsleden hun invloed op de Europese besluitvorming te onderschatten. Het ontbreekt daardoor aan afdoende parlementaire controle op die besluitvorming.

Aanbevelingen

1 Verbeter het toezicht op opsporings- en veiligheidsdiensten

De politiek mist het zicht op het gebruik door opsporings- en veiligheidsdiensten van hun bevoegdheden. Een debat over een proportionele inzet van middelen als datamining of DNA-onderzoek vergt meer inzicht in de schaal waarop en de situaties waarin deze middelen worden ingezet; welke successen ermee worden geboekt in de strijd tegen misdaad en terreur; en met welke risico's op 'mismatches' dat gepaard gaat.

2 Zet de architectuur van datasystemen op de politieke agenda

Datasystemen als het Burgerservicenummer, de nationale DNA-databank of het Schengen Informatie Systeem kampen met bestandsvervuiling, identiteitsdiefstal en slordig beheer. Het is niet duidelijk hoe deze systemen tegen deze risico's kunnen worden beveiligd. Omdat de risico's samenhangen met de omvang van datasystemen, spelen vragen over de architectuur ervan een belangrijke rol. Moeten data centraal of zoveel mogelijk decentraal worden opgeslagen? Welke koppelingen tussen bestanden zijn gewenst? Wie heeft toegang tot de gegevens? En moeten datasystemen worden gebouwd op maximale datavergaring of juist op dataminimalisatie?

3 Kijk kritisch naar de beroepsmogelijkheden voor burgers

Bestandsvervuiling, identiteitsdiefstal en foutieve interpretaties van gegevens leiden tot vals positieve uitkomsten. Hierdoor worden mensen ten onrechte verdacht van (potentieel) criminele of terroristische activiteiten. Burgers lijken over weinig mogelijkheden te beschikken zich daartegen te verweren. Dat geldt zowel voor nationaal als Europees niveau. De rechtsbescherming van burgers lijkt dan ook geen gelijke tred te houden met de politiële en justitiële bevoegdheidsverruimingen van de afgelopen jaren. Dat roept de vraag op of die rechtsbescherming geen versterking behoeft.

Relevante publicaties en activiteiten Rathenau Instituut

Vedder, A., L. van der Wees, B.J. Koops en P. de Hert, 'Van privacyparadijs tot controlestaat? Misdaad- en terreurbestrijding aan het begin van de 21ste eeuw', Studie 49, Den Haag: Rathenau Instituut, 2007

Hof, Ch. van 't, E. van den Heuvel, R. van Est en F. Brom, 'RFID: Helderheid over opsporing verzocht', Bericht aan het Parlement, Den Haag: Rathenau Instituut, 2007

Munnichs, G., A. Kets en P. Breitbarth, 'Kansen en risico's van moderne opsporingsmethoden. Discussienotitie expertbijeenkomst Gegevensbescherming', Den Haag: Rathenau Instituut, 2008

'Verslag van de expertbijeenkomst over gegevensbescherming van de vaste commissie voor Justitie van de Eerste Kamer op donderdag 20 maart 2008', Eerste Kamer, vergaderjaar 2007-2008, 31 200 VI, F

'Nederland Controlestaat? Een politiek debat over veiligheid en privacy', Amsterdam: De Balie, 17 november 2006 (www.debalie.nl)

'Little Sister versus Big Brother', Privacyproject Holland Doc (www.privacyproject.nl)

'Het Glazen Lichaam', Technologiefestival Rathenau Instituut en NRC Handelsblad, Rotterdam, 2 februari 2008 (www.hetglazenlichaam.nl)

COLOFON

Dit Bericht aan het Parlement is een uitgave van het Rathenau Instituut.

Het Rathenau Instituut laat de invloed van wetenschap en technologie op ons dagelijks leven zien en brengt de dynamiek ervan in kaart; door onafhankelijk onderzoek en debat.

Tekst
Geert Munnichs

Eindredactie
Pascal Messer en Tijs Heesterbeek

Projectteam
Geert Munnichs en Anne Kets

Fotografie
Hollandse Hoogte
iStockphoto

Basisvormgeving
Smidswater, Den Haag/Breda

Vormgeving
Max Beinema

Productie
Herbschleb & Slebos, Monnickendam

Drukwerk
Veenman Drukkers, Rotterdam

Redactieadres:
Postbus 95366 2509 CJ Den Haag
Telefoon (070) 342 15 42
e-mail info@rathenau.nl
www.rathenau.nl