

# Privacy en Mensenrechten in 70 landen

## Samenvatting onderzoeksrapport

30/10/2006

In dit jaarlijkse rapport van het Electronic Privacy Information Center en Privacy International wordt beoordeeld hoe het met de privacy is gesteld in meer dan 70 landen. De privacywetgeving wordt besproken en belangrijke kwesties en gebeurtenissen met betrekking tot privacy en toezicht komen aan de orde. De landenrapporten behandelen het grondwettelijk kader en de wet- en regelgeving met betrekking tot privacybescherming alsmede het toezicht op gegevensuitwisseling door rechtshandhavers, nieuwe, baanbrekende rechtszaken, de meest opvallende bijdragen van niet-gouvernementele organisaties en mensenrechtenorganisaties, diverse nieuwe ontwikkelingen en belangrijke privacygerelateerde nieuwsitems.

Veel ontwikkelingen in dit verslag zijn een gevolg van de behoefte van overheden aan betere beveiliging na de terroristische aanslagen van de laatste jaren in Azië, Europa, het Midden-Oosten en de Verenigde Staten. Veel landen uit alle delen van de wereld hebben ingezet op beleids- en wetgevende maatregelen gericht op het intensiveren van het overheidstoezicht op personen. Dit heeft geleid tot de invoering of verheviging van identificatiecontroles en het bijhouden van de privécommunicatie van personen. Tegelijkertijd hebben overheden halsstarrig geprobeerd aan de ene kant gegevensbeschermende maatregelen af te zwakken en aan de andere kant het verzamelen van informatie uit publieke en private bronnen te intensiveren en die informatie te delen met een groeiend aantal opsporingsinstanties en nationale veiligheidsdiensten.

### 1. Antiterrorismemaatregelen van de overheid

De meeste regeringen hebben hun inspanningen op het gebied van bewaking en controle verhoogd, met als rechtvaardiging de strijd tegen het terrorisme. Een van de belangrijkste trends is de bredere toepassing van maatregelen die de identificatie van personen die landsgrenzen passeren moeten waarborgen. In het kielzog van de Verenigde Staten hebben veel landen hun eigen versies geproduceerd van biometrische reisdocumenten die machinaal uitleesbaar zijn of passagiers-screeningssystemen op basis van nieuwe technologieën, bijvoorbeeld systemen voor de herkenning van vingerafdrukken, het maken van irisscans, gezichtsherkenning of radio frequentie identificatie (RFID). Op deze wijze scheppen veel landen de voorwaarden voor het invoeren van nationale identificatiesystemen en biometrische databases die, hoewel oorspronkelijk bedoeld voor buitenlandse bezoekers, waarschijnlijk ook zullen worden gebruikt voor minderheden toegepast en later voor alle burgers.

Dit verslagjaar hebben regeringen zich ingezet voor het invoeren van nieuwe maatregelen als antwoord op de terrorismedreiging. Sommige maatregelen zijn aangenomen voor rechtsgeldige doeleinden, andere om opsporingsdiensten nieuwe bevoegdheden te verlenen. Die bevoegdheden komen niet overeen met de oorspronkelijke, specifieke doelstelling om terrorisme te bestrijden maar zijn ingevoerd en vervolgens toegepast voor andere doeleinden. Sommige nieuwe wetten verlenen overheidsdiensten meer controlerende bevoegdheden en meer bevoegdheden om informatie van inlichtingendiensten uit te wisselen, andere zijn bedoeld om nieuwe overheidsdiensten in het leven te roepen die specifiek zijn gericht op het bestrijden van terrorisme. Het hierdoor in het leven geroepen toezicht blijkt echter vaak ontoereikend. De laatste tijd lijken overheden er dan ook in toenemende mate toe te gaan informatievergaring en -opslag uit te besteden aan particuliere ondernemingen.

### 2. Overige overheidsmaatregelen

Overheden hebben zich niet beperkt tot het nemen van nieuwe controlemaatregelen als directe reactie op de terrorismedreiging. De belangstelling voor controlerende systemen is de laatste tijd uitgebreid

tot biometrische systemen, smartcards, databases met medische gegevens, data mining en videobewakingssystemen. In de meeste landen heeft de overheid haar toevlucht gezocht tot videobewakingstechnologie voor diverse doeleinden betreffende de openbare veiligheid en rechtshandhaving, zoals het bewaken van openbare ruimten en transportmiddelen en tolheffing.

Tegenwoordig maken steeds meer overheden gebruik van smartcards voor allerlei toepassingen, van paspoorten, rijbewijzen en bankpasjes tot medische smartcards. Soms zijn ze gekoppeld aan biometrische gegevens, zodat de houders elektronisch kunnen communiceren met overheidsdiensten en gebruik kunnen maken van e-governmentdiensten. Dergelijke smartcardsystemen lijken in eerste instantie te zijn ingevoerd voor minderheden, zoals vluchtelingen en illegale buitenlanders, maar sommige landen zijn van plan de technologie later ook in te voeren voor de hele bevolking. De kritiek is veelal gericht op het ontbreken van adequate wetgeving op het gebied van de bescherming van persoonsgegevens in die landen waar deze systemen worden gebruikt en op het verhoogde risico van identiteitsdiefstal.

De afgelopen jaren is het aantal DNA-databases en databases met verschillende soorten medische gegevens gestaag toegenomen. Ze worden steeds vaker en op steeds grotere schaal gebruikt: het aantal geregistreerde misdrijven en personen zal toenemen, de bewaartermijnen worden over de gehele linie langer, opsporingsinstanties zullen zich er steeds meer op verlaten om strafbaarheid aan te tonen en sommige overheden zijn zelfs begonnen met het aanleggen van nationale DNA-databases. Deze databases worden ook steeds vaker gebruikt voor bijkomende doelen, van (het tegengaan van misbruik van) sociale zekerheidsvoorzieningen en medisch onderzoek tot het bewaken van de uitgaven in de gezondheidszorg. De privacy komt daarbij pas echt in het geding, als burgers niet weten wanneer ze worden onderworpen aan genetische tests of waarvoor en op welke manier de resultaten worden gebruikt. De (grond)wettigheid ervan wordt door critici betwist en ook wordt overheden verweten het grote publiek onvoldoende in te lichten.

Enkele van de onderzochte landen hebben drastische censuurmaatregelen genomen om het doen en laten van burgers te controleren, van het controleren van e-mails, het afluisteren van telefoongesprekken, het controleren van faxcommunicatie en SMS-berichten en het traceren van zoeken en surfgedrag op het internet tot het filteren van het internet, het onderscheppen van communicatie en het bewaken van internetcafés.

### 3. Bewaking door particuliere bedrijven

Over de hele wereld zijn particuliere bedrijven in de arm genomen voor diverse bewakingsdoeleinden. Radio Frequentie Identificatie (RFID) en videobewaking behoren tot de belangrijkste technieken die deze bedrijven hanteren. RFID is in het bedrijfsleven zeer in trek geraakt als een veelzijdig toepasbaar instrument voor bewaking, tracering, beveiliging en het beheer van voorraadmagazijnen en de toeleveringsketen. De investeringen in deze technologie en het aantal potentiële toepassingen ervan nemen met de dag toe, van toepassing in bibliotheken om het uitlenen van boeken te beheren tot de toepassing in betaalsystemen. RFID wordt steeds vaker aangeprezen als een effectieve methode om personen in de gaten te houden, te beginnen met de toepassing ervan op buitenlandse reizigers, gevangenen of andere minderheidsgroepen aan grenzen en in gevangenissen tot de recente toepassing in bewakingssystemen om werknemers en overheidsambtenaren op de werkplek te bewaken of om de toegang tot extra beveiligde ruimten te bewaken. Hoewel het voor veel toepassingen een geschikte technologie is, vormen sommige RFID-toepassingen een verhoogd risico voor de privacy van burgers, met name waar de technologie het mogelijk maakt consumenten en politieke activisten uitgebreid en heimelijk in de gaten te houden. Enkele wetgevers, overheidsdiensten en privacytoezichthouders buigen zich nu over de implicaties ervan voor de privacy van burgers en actiegroepen hebben het grote publiek inmiddels bewuster gemaakt van de risico's van de technologie voor de privacy.

Hoewel het gebruik van videobewaking door particuliere bedrijven het afgelopen jaar wereldwijd verder is toegenomen en videobewaking in steeds meer situaties wordt toegepast, hebben slechts enkele landen daarop gereageerd met maatregelen gericht tegen misbruik daarvan.

De strijd tegen ongewenste, commerciële e-mails (spam) heeft veel landen ertoe gebracht nieuwe wetten aan te nemen. In andere landen en staten zijn wetsvoorstellen daartoe in behandeling. Meer

EU-landen hebben de E-Richtlijn (Richtlijn betreffende Privacy en Elektronische Communicatie) omgezet in nationaal recht. Deze richtlijn vormt tot nu toe de belangrijkste wetgevende maatregel om te komen tot een uniforme, wettelijke aanpak van het probleem van spam. Ook andere maatregelen tegen spam worden overwogen. Het afgelopen jaar hebben internationale organisaties en overheden hun inspanningen opgevoerd om de samenwerking op het gebied van opsporing en vervolging te bevorderen, technische oplossingen te bedenken en in te voeren en het publiek te informeren. Tegelijk zijn wereldwijd diverse anti-spam organisaties, deskundigenfora en stuurgroepen opgericht om de belangen van hun achterban te behartigen. Uitspraken in belangrijke rechtszaken hebben de inbreuk op de privacy door spam verder beperkt. Diverse privacytoezichthouders hebben ook gerapporteerd dat de meeste klachten die ze ontvingen betrekking hadden op spam.

Veel Amerikaanse bedrijven die gegevens verzamelen over consumenten en internetgebruikers en vervolgens aan derden verkopen, hebben, daartoe wettelijk verplicht, gemeld dat ze te lijden hebben gehad van ernstige inbreuken op de gegevensbeveiliging. Deze gevallen toonden aan dat aan de verwerking van gegevens buiten een strikt omlijnd kader dat toeziet op de bescherming van gegevens, hoge risico's zijn verbonden en dat het noodzakelijk is gepaste veiligheidsmaatregelen te nemen. Deze inbreuken hebben ook geleid tot een sterk verhoogd risico van identiteitsdiefstal in de komende jaren en hebben het vertrouwen van internetgebruikers in e-commercebedrijven danig ondermijnd. Hoewel de gemelde gevallen van misbruik van persoonsgegevens vooral de Verenigde Staten betroffen, heeft het wanbeheer van deze commerciële gegevensverzamelaars wereldwijd gevolgen gehad, zoals mag blijken uit de oproep van wetgevers om de wetgeving op het gebied van gegevensbescherming en -beveiliging aan te scherpen. Sommige landen in de Derde Wereld hebben met name in de verwerkingsindustrie ook te maken gehad met gevallen van fraude en identiteitsdiefstal.

#### 4. Nieuwe wetgeving op het gebied van de bescherming van persoonsgegevens

Wereldwijd zijn nieuwe wetten ingevoerd en vele wetsvoorstellen ingediend om het recht van burgers op privacy en de bescherming van hun persoonsgegevens te waarborgen. In de 25 landen van de EU is de wetgeving op het gebied van de bescherming van persoonsgegevens nu geharmoniseerd. Van de overige landen die bezig zijn met het opstellen en invoeren van privacywetgeving bevinden zich de meeste in Azië en Latijns-Amerika. Over het algemeen volgen ze op het gebied van gegevensbescherming het EU-model. Vorig jaar werd in de landen van de uitgebreide EU de hierboven genoemde E-richtlijn aangenomen die internet- en telecommunicatiegebruikers bescherming biedt tegen spam en de inbreuk op vertrouwelijke communicatie.

#### 5. Succesvolle strijd van mensenrechtenorganisaties en niet-gouvernementele organisaties tegen schending van privacy

In diverse landen hebben mensenrechtenorganisaties zich krachtig gekeerd tegen inbreuken op de privacy. In Australië hebben voorvechters van de burgerlijke vrijheden een voorstel van de regering om een uitgebreide database aan te leggen op basis van volkstellinggegevens in de kiem gesmoord. In Maleisië hebben de Human Rights Caucus of the Parliament en een groep verontruste burgers zich verzet tegen staatstoezicht op het naleven van de godsdienstige zeden en gebruiken door aan te voeren dat dit een inbreuk betekende op de persoonlijke levenssfeer en integriteit van burgers. Als reactie daarop heeft de regering Islamitische overheidsinstellingen opgedragen toestemming van de politie te vragen alvorens invallen te doen bij moslims op verdenking van immoreel gedrag. In Thailand verzocht de politie de regering onlangs een wet aan te nemen die het mogelijk maakt zonder bevelschrift en zonder wettelijk toezicht telefoons af te tappen en huiszoekingen te doen. De oppositie veroordeelde deze poging om de burgerlijke vrijheden en mensenrechten aan te tasten en de regering gaf geen gevolg aan de oproep van de politie. In de Verenigde Staten werd het "CAPPS II" screening systeem na jarenlang verzet van burgerrechtenorganisaties tegen de plannen van de regering om passagiers te screenen verijdeld.

#### 6. Ontwikkelingen op het gebied van openbaarheid van bestuur

Dit jaar betroffen de meeste ontwikkelingen op het gebied van openbaarheid van bestuur nieuwe wetten of wettelijke bepalingen (Ecuador, Macedonië, Oeganda), wetsvoorstellen (Duitsland, Guatemala, Mongolië, Nigeria, Sri Lanka) en jurisprudentie met betrekking tot de bescherming van het recht op toegang tot overheidsinformatie (bijvoorbeeld Costa Rica), terwijl in het Verenigd Koninkrijk de Freedom of Information Act uiteindelijk volledig werd ingevoerd.

#### 7. Maatregelen van internationale gouvernementele organisaties

De maatregelen van internationale gouvernementele organisaties hebben zich grotendeels aan het oog van het grote publiek onttrokken, hoewel ze wel degelijk van invloed zijn op het beleid ten aanzien van de strijd tegen het terrorisme. Deze organisaties zijn bijzonder actief geweest – zonder enige democratische verantwoording te hoeven afleggen - met het ontwikkelen van antiterreurmaatregelen die van invloed zijn geweest op het nationale debat over wetgeving en beleid in de strijd tegen het terrorisme. De Raad van de Europese Unie bijvoorbeeld dringt voortdurend aan op het invoeren van nieuwe antiterrorismemaatregelen met als doel harmonisatie van de wetgeving in de lidstaten die meer bevoegdheden aan opsporingsinstanties moet toekennen zonder daaraan gekoppelde toezichts- en privacywaarborgen.

