

Bericht aan het Parlement

OKTOBER 2007

**RFID: helderheid over
opsporing verzocht** 1

RFID ter discussie 2

Hoe werkt RFID? 3

**Het maatschappelijk
draagvlak voor RFID
als opsporingsmiddel** 3

**Met het nieuwe paspoort
naar een biometrische
database voor opsporing?** 6

**Met de OV-chipkaart
naar opsporing met
reizigersgegevens?** 8

**Dataretentie:
hoge kosten,
rem op innovatie** 10

**Naar een integrale visie
over RFID, privacy,
opsporing en innovatie** 11

Aanbevelingen 11

Referenties & publicaties 12

RFID: Helderheid over opsporing verzocht

Een ruime meerderheid van de Nederlanders vindt het goed dat de digitale vingerafdrukken en foto's uit het nieuwe biometrische paspoort worden gebruikt voor de opsporing van getuigen en verdachten. Ook de reizigersgegevens van de nieuwe OV-chipkaart mogen hiervoor worden gebruikt, zo blijkt uit een gezamenlijk onderzoek van het Rathenau Instituut, de Consumentenbond en ECP.nl. Het paspoort en de OV-chipkaart zijn twee voorbeelden van RFID (*Radio Frequency Identification*): op afstand uitleesbare chips die elke dag en door iedereen gebruikt worden voor betaling, toegang en identificatie. Wordt RFID het nieuwe wapen in de criminaliteitsbestrijding?

De Tweede Kamer discussieerde vaak en fel over RFID en het bedrijfsleven. Vooral over de vraag hoe de overheid consumentenprivacy kan waarborgen zonder de technologische innovatie af te remmen. Maar over het gebruik van RFID-data voor opsporingsdoeleinden blijft het stil.

Het Rathenau Instituut adviseert met dit Bericht aan het Parlement:

1 het ministerie van Binnenlandse Zaken helderheid te scheppen over het doel van centrale opslag van de biometrische gegevens van het RFID-paspoort. Wordt het mogelijk en is het wenselijk dat deze gebruikt gaan worden voor opsporingsdoeleinden?

2 het ministerie van Verkeer en Waterstaat een standpunt in te nemen over het gebruik van reisgegevens van de OV-chipkaart. Worden deze centraal opgeslagen? Is het mogelijk en wenselijk dat deze gebruikt worden voor opsporing?

3 het ministerie van Justitie onderzoek te starten naar de effectiviteit van RFID als opsporingsmiddel.

4 het ministerie van Economische Zaken aan te geven of de wetgeving rondom dataretentie (verplicht bewaren van data voor opsporingsdoeleinden) ook voor RFID-data gaat gelden.

5 de overheid tot een interdepartementale visie over RFID te komen, met daarin aandacht voor het evenwicht tussen innovatie, privacy en opsporingsbelangen.

RFID ter discussie

Betalen bij het Shell-station, punten sparen voor de volgende AZ-wedstrijd, de kantoordeur die zich voor u opent: RFID is overal. Handeling, tijd en plaats worden geregistreerd. In het debat onder experts, belanghebbenden en Kamerleden komt privacy daarom regelmatig aan bod. De vraag hoe het bedrijfsleven moet omgaan met RFID-toepassingen staat centraal: Welke gegevens mogen er wel of niet verzameld worden? Waar mogen ze voor worden gebruikt? Hoe moeten ze worden beveiligd? Wat moet de consument hierover weten? Voldoet de Wet Bescherming Persoonsgegevens?

Dit zijn belangrijke vragen. Maar de rol van de opsporingsdiensten bij de gegevensverzameling komt hierbij nauwelijks aan bod. Uit de Rathenau Instituut-studie *'Van privacyparadijs tot controlestaat?'* van februari 2007, blijkt dat de opsporingsbevoegdheden en technische mogelijkheden van politie en justitie de afgelopen tien tot vijftien jaar drastisch zijn uitgebreid. Welke nieuwe mogelijkheden biedt RFID voor opsporing? En valt de benutting van deze technologie binnen de bevoegdheden?

Om deze vragen helder te krijgen, organiseerden het Rathenau Instituut en ECP.nl daarom in april 2007 het publieke debat 'RFID, opsporing en privacy.' Aanwezig waren het College Bescherming Persoonsgegevens (CBP), kamerleden van de vijf grootste partijen en vertegenwoordigers van Philips en KPN. Harm Brouwer, voorzitter van het College van procureurs-generaal, zette de visie van het Openbaar Ministerie uiteen: voor opsporingsdiensten zijn RFID-gegevens zeker interessant.

De discussie onder de Kamerleden richtte zich op de wenselijkheid van RFID voor opsporing.

De tegenstelling tussen privacy en veiligheid kwam daarbij scherp aan het licht. Het ene kamp stelde dat opsporing buiten het oorspronkelijke doel van RFID ligt, terwijl anderen juist stelden dat privacy te vaak een dekmantel is voor criminelen. RFID is voor hen een welkome aanvulling in het opsporingsarsenaal. De bedrijven, KPN en Philips, en de overheidsorganisaties vroegen vooral om duidelijkheid: moeten wij bij de aanleg van onze systemen nu al rekening houden met opsporingsbelangen?

Op dit moment worden er twee RFID-systemen aangelegd die de discussie urgent maken: het biometrisch paspoort en de OV-chipkaart. Mogen de biometrische gegevens die nu op de RFID-chip van het paspoort staan, in de toekomst ook centraal worden opgeslagen voor opsporingsdoeleinden? Met een centrale database kunnen met vingerafdrukken of camerabeelden van een plaats van delict, verdachten of getuigen worden geïdentificeerd. Met de OV-chipkaart wordt geregistreerd wanneer en waar reizigers zich in het openbaar vervoer bevinden.

"Wij – en daarmee bedoel ik de politie en het OM – krijgen nogal eens het verwijt, dat wij steeds om nieuwe bevoegdheden roepen. Welnu, voorzover ik het nú kan overzien, biedt de huidige wetgeving inzake strafvorderlijke gegevensvergaring ons voldoende bevoegdheden om – wanneer dat noodzakelijk is voor de opsporing – RFID –informatie op te vragen."

Harm Brouwer, voorzitter van het College van procureurs-generaal



Het maatschappelijk draagvlak voor RFID als opsporingsmiddel

Hoe werkt RFID?



Een RFID-systeem bestaat uit vier elementen:

RFID-chips, chiplezers, een netwerk en meestal een database.

Die elementen wisselen informatie uit. Als de chip dicht genoeg bij een chiplezer komt, geeft hij zijn code af. Bij de meeste toepassingen wordt die code gebruikt om informatie te ontsluiten uit een database. Bij de OV-chipkaart staan naast de unieke code ook het betaaltgeod en (bij gepersonaliseerde kaarten) de leeftijd van de kaartdrager erop.

Op de chip van het biometrisch paspoort wordt ook een digitale foto opgeslagen. De Rathenau Special "RFID: meer keuze, gemak en controle in de digitale publieke ruimte" uit april 2007 geeft een overzicht van RFID-toepassingen in het leven van alledag.

Deze zomer onderzochten het Rathenau Instituut, de Consumentenbond en ECP.nl wat de Nederlandse bevolking weet en vindt van RFID. Dit onderzoek bestond uit vier publiekspanels en een landelijke enquête onder tweeduizend Nederlanders. Slechts een minderheid is bekend met de term RFID (39 procent). Toch gebruikt vrijwel elke Nederlander (98 procent) één of meerdere RFID's: een kantoortpas, een chip in het huisdier, een OV-chipkaart of biometrisch paspoort. En al roept de term bij menigeen in eerste instantie een 'Big Brother-gevoel' op, een meerderheid ziet vooral voordelen in de controlemogelijkheden van RFID. Bij vragen over RFID-data voor opsporing is een breed draagvlak voor de inzet ervan. Bij het biometrisch paspoort en de OV-chipkaart is de verhouding over het algemeen 60 procent voor en 20 procent tegen inzet van RFID voor opsporing (zie pagina 4 en 5).

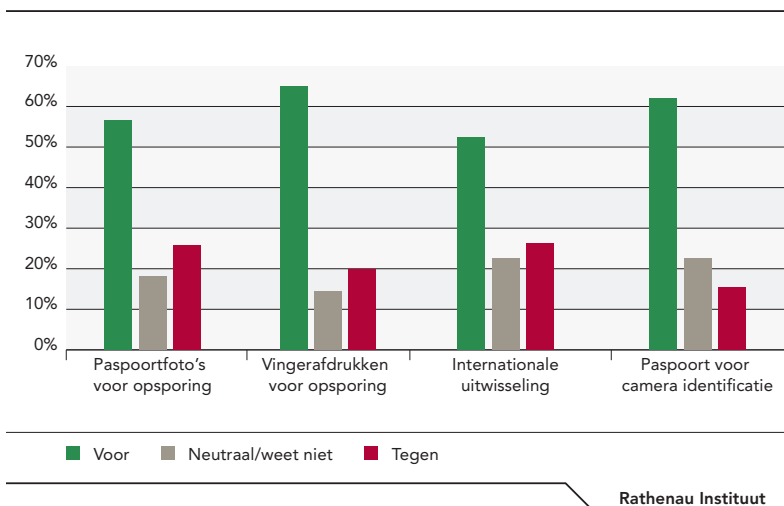


Biometrische data voor opsporingsdoeleinden

Hoe denkt de Nederlandse bevolking over het digitaliseren van biometrische gegevens voor het paspoort? 74 procent is bekend met het biometrisch paspoort. Van degenen die er al een had (23 procent), bleek slechts 30 procent geïnformeerd te zijn over de foto op de chip. De toevoeging van een vingerafdruk stuit vooralsnog op weinig weerstand: slechts 6 procent is tegen.

We legden de respondenten een hypothetisch scenario voor waarin de biometrische gegevens centraal in een database worden opgeslagen voor opsporingsdoeleinden. Ze konden daarbij aangeven of zij voor of tegen het gebruik van pasfoto's en vingerafdrukken voor opsporingsdoeleinden zijn. Ook vroegen we of de pasfoto's gebruikt mogen worden voor cameraherkenning, en of de verzamelde reisgegevens voor terrorismebestrijding mogen worden uitgewisseld met andere landen.

Figuur 1 Draagvlak voor opsporing met paspoortdata in één database



Deze figuur laat zien dat een meerderheid vóór dergelijke maatregelen is. Hier moet wel de kanttekening bij worden geplaatst dat niet iedereen vooraf wist wat het biometrisch paspoort is en dus op basis van beperkte informatie besliste. Opmerkelijk genoeg bleek het vertrouwen in de technologie laag. Liefst 68 procent van de respondenten is van mening dat het een kwestie van tijd is totdat ook dit nieuwe paspoort na te maken is. Slechts 1 procent dacht dat het onmogelijk is om het nieuwe paspoort na te maken.

Reizigersgegevens voor opsporingsdoeleinden

De OV-chipkaart geniet iets meer bekendheid, maar minder gebruikers onder de bevolking: 89 procent kent de kaart, 7 procent heeft hem al. Van hen heeft 80 procent een persoonlijke kaart.

De ervaringen met de kaart zijn voornamelijk positief. Van de mensen die de kaart nog niet hebben, maar wel willen, kiest 37 procent in eerste instantie voor een anonieme kaart. Als de gepersonaliseerde kaart financiële voordelen geeft, kiest 87 procent toch voor een persoonlijke variant.

Om het draagvlak voor opsporing met het OV-Chip-systeem te onderzoeken, legden we de respondenten voor of de reizigersgegevens gebruikt mogen worden voor het opsporen van getuigen of verdachten van een misdrijf. Ook legden we een denkbeeldig scenario van een volledig gepersonaliseerd openbaar vervoer voor. De respondenten konden daarbij aangeven of zij het eens zijn met de stelling: 'Iedereen zou een persoonsgebonden OV-chipkaart moeten hebben, zodat mensen die zich misdragen, geweerd kunnen worden uit het openbaar vervoer.' Figuur 2 toont een draagvlak voor de OV-chipkaart als opsporingsmiddel dat overeenkomt met dat van het biometrisch paspoort. De verhoudingen komen overigens overeen met de gegevens uit de honderd reizigersinterviews die het Rathenau Instituut in januari 2007 liet verrichten.

Vertrouwen in technologie en overheid

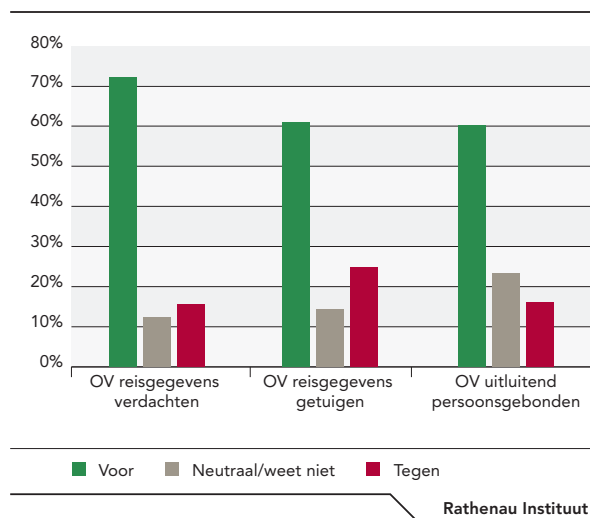
We legden de respondenten ook een lijst met voor- en nadelen van RFID voor. Zij werden gevraagd aan te geven welke zij het belangrijkste vonden. Als voordeel scoorde 'criminaliteitsbestrijding' het hoogst. Het 'gemak' kwam op de tweede plaats en het voordeel 'Identiteit is beter vast te stellen', op de derde. Ook hieruit blijkt dat er maatschappelijk draagvlak voor het gebruik van RFID-gegevens voor opsporing is. Op de vraag welke nadelen van RFID de respondenten het belangrijkste vinden, stond niet het privacyargument bovenaan bij de beantwoording, maar het nadeel 'Als het systeem een fout maakt, kun je dat moeilijk rechtzetten.'

Bij het beheer van de RFID-gegevens kan de overheid rekenen op een redelijk vertrouwen onder de bevolking: 51 procent heeft veel tot zeer veel vertrouwen in de overheid, tegenover 18 procent 'weinig' tot 'geen' vertrouwen.

De hang naar controle ten koste van privacy, is ook terug te vinden in andere recente onderzoeken. Uit het Nationaal Vrijheidsonderzoek 2007 van het Nationaal Comité 4 en 5 mei bleek bijvoorbeeld dat de groep respondenten die denkt dat de veiligheid toeneemt als de overheid meer over burgers weet, groter is dan de groep die dat niet vindt. Strengere veiligheidsmaatregelen worden daarbij niet gezien als grote bedreiging voor de persoonlijke vrijheid. Ook hebben het CBP en TNS-NIPO een aantal groeps-



Figuur 2 Draagvlak voor opsporing met de OV-chipkaart



gesprekken gevoerd waaruit bleek dat respondenten laconiek omgaan met hun persoonsgegevens: *'Ik heb toch niets te verbergen; als het misdaden voorkomt, zeg ik "iedereen mag alles van me weten".'*

Enige kanttekeningen bij het onderzoek dat het Rathenau Instituut samen met de Consumentenbond en het ECP.nl deed, zijn op hun plaats. Ten eerste zijn nog maar weinig mensen zich ervan bewust wat RFID eigenlijk inhoudt. Naarmate men er meer van te weten komt, kunnen deze cijfers wijzigen. Bij sommige vragen bleek bijvoorbeeld dat mensen die wel bekend waren met de term RFID, minder

'Een meerderheid ziet vooral voordelen in de controle-mogelijkheden van RFID'.

geneigd waren mee te gaan in opsporingsdoeleinden. De stelling *'Het maakt mij niet uit dat er RFID-gegevens over mijn gedrag verzameld worden, "ze" weten al heel veel van mij.'* kon niet op een meerderheid rekenen (37 procent). Een andere bedenking die we veel tegenkwamen in de focusgroepen: men vertrouwt weliswaar de huidige overheid op correct gebruik van hun RFID-data, maar vreest wel dat een toekomstige of een buitenlandse overheid (de VS) dat misschien niet doet.

Het volledige rapport:

"RFID-bewustzijn van consumenten: Hoe denken Nederlanders over Radio Frequency IDentification?" is digitaal verkrijgbaar op www.rathenau.nl.

Voor meer over de publieke beleving van privacy zie: www.privacyproject.nl met films, documentaires, weblogs en ruimte voor een eigen profiel.



Met het nieuwe paspoort naar een biometrische database voor opsporing?

Sinds 26 augustus 2006 hebben alle nieuwe Nederlandse paspoorten een RFID-chip met digitale pasfoto.

Volgens planning worden vanaf 2009 ook twee vingerafdrukken op de chip opgeslagen. De belangrijkste reden hiervoor is het voorkomen van identiteitsfraude: het paspoort is zo moeilijker te vervalsen en de digitale gelaatsscan is beter te verifiëren.

Op dit moment worden die data decentraal opgeslagen bij de paspoortuitgevende instantie. Sdu Uitgevers, die de paspoorten maakt, is vooralsnog de enige plek waar de data samenkomen.

Het Agentschap Basisadministratie Persoonsgegevens en Reisdocumenten werkt aan ORRA: de Online Raadpleegbare Reisdocumenten Administratie. Dit is een centrale database waar paspoortuitgevende instanties bij een aanvraag kunnen controleren of de door de aanvrager opgegeven gegevens juist zijn, en of de aanvrager onder een andere identiteit al in het bezit is van een Nederlands reisdocument. Volgens Guus Rutgers, directeur van het Agentschap, is deze verificatie ter voorkoming van duplicatie het enige doel van de gegevenscentralisatie. Echter, één database met zowel de digitale gelaatsscan als de vingerafdruk van



elke paspoorthouder, biedt interessante mogelijkheden voor opsporings-ambtenaren. De vingerafdrukken en pasfoto's zijn immers zodanig gedigitaliseerd en opgeslagen dat gezocht kan worden naar overeenkomsten. Camera-beelden en vingerafdrukken van de plaats van een misdrijf zouden dan ook vergeleken kunnen worden om verdachten en getuigen te achterhalen. Als de dader een biometrisch paspoort heeft, dan staan ook zijn gegevens in de database.

Over een dergelijke uitbreiding van de oorspronkelijke functie van het paspoort is in het verleden slechts kort gesproken in de Tweede Kamer. Atzo Nicolaï - tijdens de invoering vorig jaar augustus de verantwoordelijke minister - stelde in reactie op mediaberichten dat er geen sprake zou zijn van een 'biometrische database'. Dat, terwijl ORRA toen wel al op de begroting van Binnenlandse Zaken stond. Het Agentschap heeft het voorstel voor de database deze zomer naar de Eerste Kamer gestuurd. Op dit moment ligt het bij de Raad van State voor advies. Wordt ORRA de biometrische database voor opsporing of niet? Dat is een politieke vraag.

Overwegingen

Stel, de biometrische database krijgt een opsporingsdoel. De overheid zal dan vooraf goed moeten nadenken over de volgende kwesties:

- Is het aanvaardbaar om biometrische gegevens te gebruiken van de paspoorthouders die nu al die gegevens hebben afgestaan, maar niet zijn ingelicht over deze doeluitbreiding?
- Volstaat de huidige Wet bevoegdheden vorderen gegevens om ongeoorloofd gebruik te voorkomen?
- Bij welke strafmaat krijgt de politie toegang tot de database? Bij verdenking van moord, of ook bijvoorbeeld bij winkeldiefstal?
- Mag deze database ook gebruikt worden voor preventieve opsporing en *datamining* op basis van risicoprofielen, zoals momenteel gebeurt bij terrorismebestrijding?
- Hoe effectief is het gebruik van de database voor opsporing? Wat is de kans dat de biometrische gegevens van twee verschillende personen toch matchen (vals-positieven)? Hoe zullen criminelen reageren? Gaan zij bijvoorbeeld, nog meer dan voorheen, her en der vingerafdrukken van anderen op de plaats van de misdrijf verspreiden?



Met de OV-Chipkaart naar opsporing met reizigersgegevens?

Op dit moment wordt de OV-chipkaart ingevoerd als betaalsysteem in tram, trein, metro en bus. Volgens de huidige planning zal in 2009 het openbaar vervoer in heel Nederland uitsluitend te benutten zijn met deze RFID-kaart. De uitleesapparatuur bij de bus- en tramchauffeurs en trein- en metrotourniquets registreren dan elke reiziger die in- en uitstapt. Een deel van hen reist anoniem. Maar, zoals uit ons publieksonderzoek blijkt, is dat waarschijnlijk een minderheid.

Tijdens het seminar 'RFID, opsporing en privacy', stelde voorzitter van het College van procureurs-generaal, Harm Brouwer, het volgende: "Die (OV-chipkaart - red) 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. Bovendien is het mogelijk om door gebruik te maken van de opnames van surveillance-camera's het uiterlijk van de kaartgebruiker in beeld te krijgen. Ook kan men op zoek gaan naar personen die mogelijk getuige zijn geweest van een misdrijf omdat ze op een bepaalde tijd op het perron moeten zijn geweest."

Brouwer kreeg bijval van de Kamerleden Jos Hessels (CDA) en Fred Teeven (VVD). Teeven voegde daaraan toe: "Als een verdachte door de tourniquets gaat, kunnen we ook kijken wie met hem meeloopt." Hij vroeg zich hardop af: "Als we nu alleen maar persoonsgebonden kaarten zouden hebben, dan kunnen we nog veel beter alle boeven uit het OV weren." Arda Gerken (SP) daarentegen, stelde dat opsporing niet het oorspronkelijke doel is van de OV-chipkaart. De kaart mag daar dan ook niet voor gebruikt worden. Ze kreeg bijval van Attje Kuiken (PvdA). Gerken betreurde het dat tijdens de vele Kamerdebatten over de kaart het onderwerp opsporing nooit aan de orde is gekomen. De SP is de enige partij die in de huidige schriftelijke ronde in de Tweede Kamer, hierover een vraag stelt aan Staatssecretaris Van Heemskerk.

Hoe realistisch is het dat een OV-kaart gebruikt kan worden voor opsporing? Bij de Londen Oyster Card -

"Die (OV-chipkaart - red) 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. Bovendien is het mogelijk om door gebruik te maken van de opnames van surveillancecamera's het uiterlijk van de kaartgebruiker in beeld te krijgen. Ook kan men op zoek gaan naar personen die mogelijk getuige zijn geweest van een misdrijf omdat ze op een bepaalde tijd op het perron moeten zijn geweest."

Harm Brouwer, voorzitter van het College van procureurs-generaal

een vergelijkbaar RFID-systeem - is dat al meerdere keren voorgekomen. De Britse krant The Guardian onthulde dat de Londense politie in de maand januari in 2006 61 keer de reizigersgegevens opvroeg, op zoek naar verdachten. Over het resultaat is echter niets bekend. Stel nu dat er in de Amsterdamse metro een moord wordt gepleegd. De politie kan dan volgens de Wet bevoegdheden vorderen gegevens alle relevante reisgegevens opvragen bij het Gemeentelijk Vervoer Bedrijf (GVB). En op basis daarvan kunnen getuigen worden opgeroepen.

De vraag is echter of met de OV-chipkaart de verdachte ook wordt gevonden. De huidige architectuur van het systeem is immers ingericht met enkele privacy-waarborgen. De dader kan een anonieme kaart hebben en is daarmee niet meer dan een nummer. Is de kaart wel persoonlijk, dan hangt het ervan af waar die kaart is aangeschaft. De readers bij de tourniquets en de centrale database van Translink Systems registreren namelijk alleen het nummer van de kaart om de transacties te doen. Heeft de dader de kaart bijvoorbeeld bij de RET in Rotterdam aangeschaft of bij de NS, dan liggen daar zijn persoonsgegevens, en niet bij het GVB. De politie moet dan Translink Systems en alle vervoersmaatschappijen vragen om alle nummers en persoonsgegevens te koppelen – iets wat bewerkelijk en tijdrovend kan blijken.

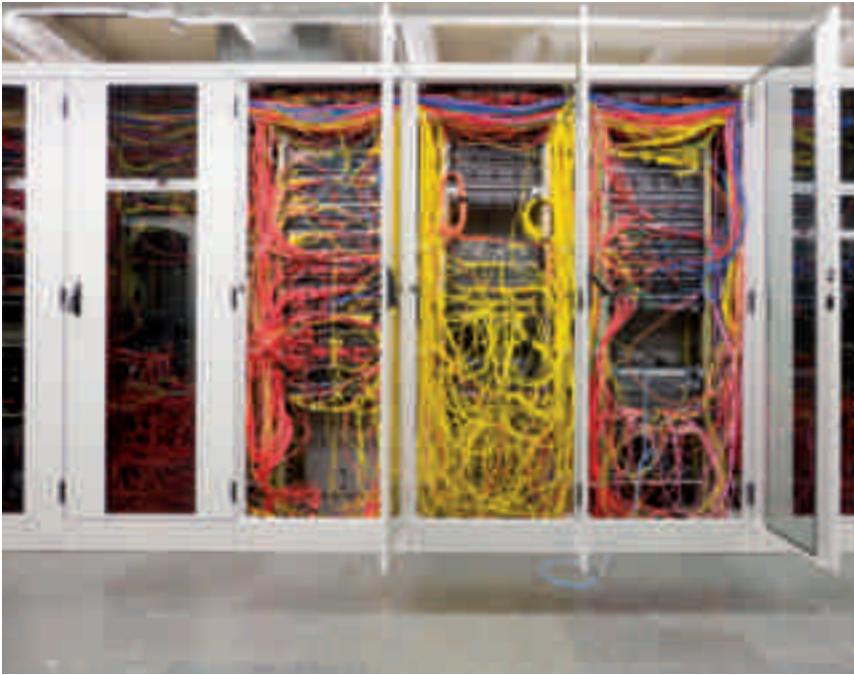
In het belang van de veiligheid kan gekozen worden voor totale personalisering en centralisering van reizigergegevens. Analoog aan het internationale vliegverkeer is dan van elke reiziger de identiteit bekend. Ook hiervoor bleek in het publieksonderzoek een redelijke meerderheid te zijn. Het is echter een politieke vraag of zo'n maatregel in verhouding staat tot het doel.



Overwegingen

- Wat is de strafmaat waarbij gegevens gebruikt mogen worden? Mogen de gegevens alleen worden opgevraagd bij een concrete verdenking van zware misdaad, of kan bijvoorbeeld ook de fiscus dit systeem gebruiken om te zien of uitkeringsgerechtigden dagelijks op vaste tijden reizen en dus wellicht toch werk hebben?
- Mag het systeem gebruikt worden voor preventieve opsporing? Bijvoorbeeld wanneer iemand reisgedrag vertoont dat lijkt op dat van een terrorismeverdachte?
- Hoe zal dit systeem de relatie tussen de openbaarvervoersbedrijven en de reizigers beïnvloeden? Voelt de reiziger zich veiliger of meer bekeken? Gaan bedrijven deze informatie ook gebruiken voor andere (marketing-)doeleinden? Hoe zal Nederland overkomen op buitenlandse reizigers als zij slechts op vertoon van hun paspoort een treinkaartje kunnen kopen?
- Gaat de Wet op de dataretentie ook gelden voor vervoersaanbieders? (Volgens deze wet moeten telecombedrijven en financiële instellingen verkeersgegevens anderhalf jaar bewaren.) Wat zijn de financiële en praktische gevolgen van het bewaren en ontsluiten van reisgegevens volgens de eisen van de politie?





Dataretentie: hoge kosten, rem op innovatie

De opkomst van RFID is onstuitbaar. 22 procent van de bevolking maakt gebruik van RFID-sleutels voor op het werk. Voetbalstadions, videotheken en fitnessclubs werken met RFID toegangs- en betaalsystemen, gekoppeld aan databases met gegevens over bestedingen en gedrag. Ook RFID in mobiele telefoons voor betaling en identificatie is in opkomst.

“Hoe intensiever bedrijven gebruik gaan maken van RFID, des te meer mogelijkheden er ontstaan voor de opsporing. Vanuit dat perspectief juicht het Openbaar Ministerie de ontwikkelingen met betrekking tot RFID alleen maar toe.”

Harm Brouwer, voorzitter van het College van procureurs-generaal

Als dan ook meer en meer producten RFID-chips gaan bevatten, bevinden we ons in een gedigitaliseerde publieke ruimte. Of, in de woorden van Harm Brouwer, voorzitter van het College van procureurs-generaal tijdens het Rathenau Instituut-publieksseminar: “Hoe intensiever bedrijven gebruik gaan maken van RFID, des te meer mogelijkheden er ontstaan voor de opsporing. Vanuit dat perspectief juicht het Openbaar Ministerie de ontwikkelingen met betrekking tot RFID alleen maar toe.”

De RFID-systemen worden niet met een opsporingsdoel aangelegd. Maar ze kunnen daar wel voor gebruikt worden. Dat gebeurde ook met mobiele telefoons en banksystemen. De EU heeft daarom een dataretentierichtlijn uitgevaardigd voor telecombedrijven, internetaanbieders en financiële instellingen, die in Nederland leidde tot wijziging van de Telecommunicatiewet en de Wet op de economische delicten. Nu moeten bepaalde data op een bepaalde manier voor anderhalf jaar bewaard worden, voor het geval ze een opsporingsdoel kunnen dienen. Het gaat dan bijvoorbeeld om wie wanneer met wie heeft gebeld en vanaf welke locatie.

De wetwijziging stuit volgens de Adviescommissie Informatiestromen op grote bezwaren bij bedrijven. Voor veel bedrijven is onduidelijk hoe de data moeten worden opgeslagen, terwijl zij ook nog eens voor de kosten opdraaien. Over de financiële gevolgen van dataretentie lopen de schattingen uiteen. Verdonck, Klooster & Associates berekenden dat deze, afhankelijk van de vorm van opslag, op een termijn van vijf jaar rond honderdvijftig miljoen euro bedragen.

Toepassing van de dataretentiewet op RFID zal grote gevolgen hebben voor de invoering ervan. Moet elke werkgever, fitnessclub of supermarkt bijhouden wie dagelijks in- en uitloopt? Gaat de wet ook gelden voor objectgebonden RFID's, zodat achteraf gekeken kan worden wie wat heeft aangeschaft? Of zal de hoeveelheid data dan simpelweg te groot worden om te bewaren, laat staan te analyseren? Hoe zal deze wetgeving de acceptatie van RFID als nieuwe technologie beïnvloeden? Nederland kent veel nieuwe, kleine bedrijven met innovatieve RFID-toepassingen. NXP (voormalig Philips) is wereldwijd de grootste producent van RFID-chips. Moet dit bedrijf straks haar klanten vertellen dat hun applicatie mogelijk-kerwijs een opsporingsdoel krijgt, met alle kosten vandien? Kortom, hier kan het opsporingsbelang haaks komen te staan op innovatie.

Naar een interdepartementale visie

Burgers en bedrijfsleven zijn gebaat bij duidelijke politieke keuzes en waarborgen. Het Rathenau Instituut schetst vier mogelijke scenario's:

Scenario 1: Heldere keuze tegen RFID als opsporingsmiddel

Kiest de overheid tegen RFID als opsporingsmiddel, dan bespaart dat een hoop extra werk bij het bedrijfsleven. Ook de onrust onder de tegenstanders wordt weggenomen. Alleen de juridische mogelijkheden die er nu al zijn om RFID als opsporingsmiddel in te zetten, moeten dan nog worden bekeken. Moet bijvoorbeeld de Wet bevoegdheden vordering gegevens worden aangescherpt?

Scenario 2: Niets regelen, maar achteraf wel RFID-data gebruiken voor opsporing

Nog afgezien van de morele vraag of het te verantwoorden is dat burgers hun persoonsgegevens hebben afgegeven voor een doel dat achteraf wordt aangepast, speelt er ook een praktisch probleem: de bestaande RFID-systemen zijn niet aangelegd met een opsporingsdoel. Het vergaren van RFID-data kan dan leiden tot veel handwerk. Of erger, tot onterechte beschuldigingen van verdachten. Eén incident kan de acceptatie van RFID totaal doen afnemen.

Scenario 3: Heldere, onderbouwde keuze vóór RFID als opsporingsmiddel

In het derde scenario wordt duidelijk gekozen voor RFID als opsporingsmiddel, en worden de benodigde technische en juridische maatregelen genomen. Bij die keuze moet dan wel de afweging worden gemaakt of het middel in verhouding staat tot het doel. Moeten bijvoorbeeld ook de bestaande RFID-systemen verbouwd worden? Gaat de Wet op dataretentie dan ook gelden voor de bedrijven die RFID toepassen? Komen er regels voor de bewaartermijn en de gegevens en de wijze waarop die bewaard moeten worden? Wie betaalt dat? Bovendien, hoe verhouden de maatregelen zich tot de bestaande privacymaatregelen (zoals decentrale opslag)?

Scenario 4: Kostbare dataretentie zonder nut

In een laatste scenario wordt gekozen voor een uitbreiding van de dataretentiewet naar RFID-data, terwijl later blijkt dat die data nauwelijks van nut blijken voor opsporing. De kosten worden dan afgewenteld op het bedrijfsleven, terwijl de innovatie en acceptatie van RFID-technologie worden afgeremd.

Conclusie:

Of nu gekozen wordt voor of tegen RFID als opsporingsmiddel, de vragen rondom het biometrisch paspoort en de OV-chipkaart maken duidelijk dat helderheid geboden is. Het is hoog tijd om te onderzoeken of RFID als opsporingsmiddel gewenst, en of het effectief is.

Aanbevelingen

1. Helderheid over de status van biometrische data

De digitale pasfoto's en vingerafdrukken van elke paspoorthouder in Nederland worden waarschijnlijk binnenkort centraal opgeslagen. Het Rathenau Instituut vraagt het ministerie van Binnenlandse Zaken helderheid te scheppen over de status van die gegevens. Is het mogelijk en wenselijk dat deze gebruikt worden voor opsporingsdoeleinden?

2. Helderheid over de status van reizigersgegevens

Reizigersgegevens, verzameld via het OV-chipkaart-systeem kunnen interessant zijn voor opsporingsdoeleinden. Het Rathenau Instituut vraagt het ministerie van Verkeer en Waterstaat helderheid te scheppen over de status van die gegevens. Worden zij centraal opgeslagen en is het mogelijk en wenselijk dat deze vervolgens gebruikt worden voor opsporingsdoeleinden?

3. Inzicht in de effectiviteit van RFID als opsporingsmiddel

RFID-data kunnen een goudmijn zijn voor opsporingsdiensten, omdat zij veel vertellen over wie, wanneer, wat en waar heeft gedaan. De vraag is echter of de kosten en moeite van de inzet van dit middel in verhouding staan tot de pakkans van eventuele verdachten. Het Rathenau Instituut adviseert het ministerie van Justitie onderzoek te starten naar de effectiviteit van RFID als opsporingsmiddel.

4. Een doordachte keuze voor of tegen dataretentie

Wordt RFID-data ingezet voor opsporing, dan kan dat worden gevolgd door een roep om uitbreiding op de wetgeving rondom dataretentie. Dit kan echter grote gevolgen hebben voor de kosten en innovatie. Het is belangrijk dat het ministerie van Economische Zaken ingaat op de vraag of de dataretentiewetgeving ook voor RFID gaat gelden.

5. Naar een interdepartementale visie over RFID, innovatie, privacy en opsporingsbelangen

Het politieke debat over RFID is momenteel verspreid over de verschillende departementen. Verkeer en Waterstaat behandelt de OV-chipkaart, Binnenlandse Zaken het paspoort, Justitie de opsporing en Economische Zaken RFID in het algemeen. We vragen de overheid te komen tot een integrale visie over RFID, innovatie, privacy en opsporingsbelangen voor alle betrokken departementen.

Rathenau Instituut publicaties over RFID in 2007

Van den Heuvel, E, Nagel, K., Van 't Hof, C en Schermer, B. *RFID bewustzijn van consumenten: Hoe denken Nederlanders over Radio Frequency Identification?* Den Haag: Rathenau Instituut, Consumentenbond en ECP.nl

Schuurman, J. et al, (Krom, A. & Walhout, B. red.) *Ambient Intelligence: Toekomst van de zorg of zorg van de toekomst?* Den Haag: Rathenau Instituut.

Hof, C. van 't & Van Est, R. *RFID: meer keuze, gemak en controle in de digitale publieke ruimte.* Rathenau Special.

Hof, C. van 't *RFID & Identity Management in the Everyday Life of European Citizens. Balancing convenience, control and choice in a new dimension of the digital public space.* (eindrapport STOA-project 'RFID & Identity Management.') Brussel: Europees Parlement.

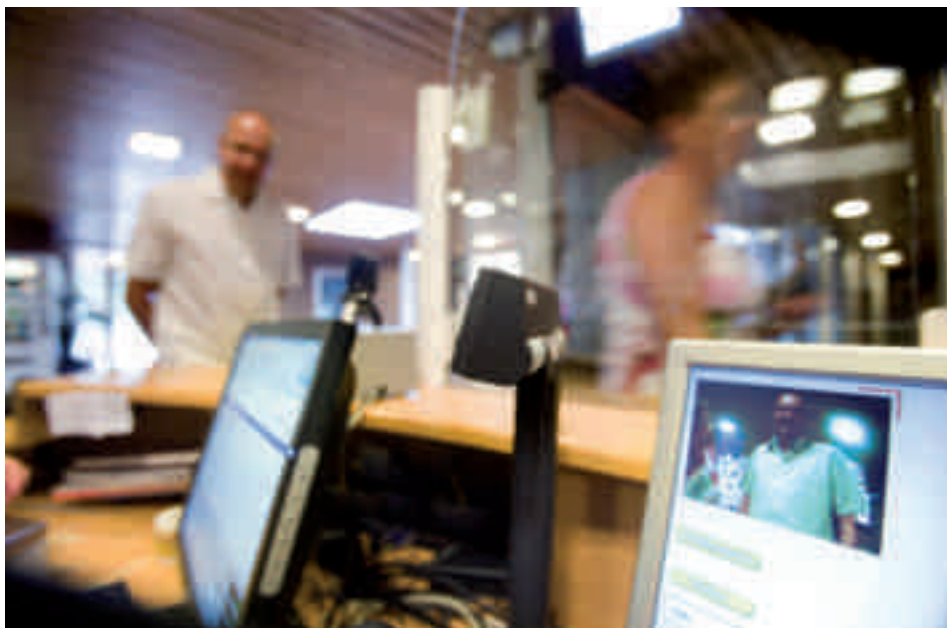
Hof, C. van 't *What do RFIDs tell about you? A user perspective on identity management* (discussiestuk STOA Workshop 'RFID in the everyday life of Europeans [...]', European Parliament, Brussel, 24 Jan. 2007

Vedder, A. ... [et al.] *Van privacyparadijs tot controlestaat? Misdaad en terreurbestrijding in Nederland aan het begin van de 21ste eeuw.* Eindred.: D. van Harten & G. Munnichs, Den Haag: Rathenau Instituut.

Verslag seminar RFID, privacy en opsporing, op 4 april 2007, Den Haag: Rathenau Instituut.

Deze publicaties en het achterliggende onderzoek zijn digitaal verkrijgbaar op: www.rathenau.nl

Voor meer informatie over RFID kunt u contact opnemen met Christian van 't Hof, e-mail: c.vanhof@rathenau.nl



Referenties

Adviescommissie Informatiestromen Veiligheid Data voor daadkracht. *Gegevensbestanden voor veiligheid: observaties en analyse*, Den Haag, 2007 (<http://www.nctb.nl/>)

Brouwer, H.N. *Speech ter gelegenheid van seminar RFID en opsporing 4 april 2007* (www.om.nl/over_het_om/speeches/31525/)

Brief van de Minister van Binnenlandse Zaken. Kamerstuk 25764, nr. 30, 31 augustus 2006

Kamerstuk 30 800 XIII (Vaststelling van de begrotingsstaten van het ministerie van Economische Zaken (XIII) voor het jaar 2007. Verslag van een schriftelijk overleg.)

Rijksbegroting ministerie van Financiën (ORRA op de Rijksbegroting) (http://rijksbegroting.minfin.nl/rijksbegroting_nl)

Verdonck, Klooster & Associates bv, *Onderzoek naar de nationale implementatie van de Europese richtlijn dataretentie* Onderzoek in opdracht van de Minister van Justitie, 2006

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

Christian van 't Hof, Eefje van den Heuvel, Rinie van Est en Frans Brom

Eindredactie

Afdeling Communicatie

Fotografie

Rathenau Instituut
Hollandse Hoogte

Vormgeving en productie

Smidswater, Den Haag/Breda

Drukwerk

Veenman Drukkers, Rotterdam

Redactieadres:

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