RFID in het opsporingsdomein

'Over twintig jaar bestaat privacy niet meer'

Kees Crone

Overheden hebben altijd interesse in informatie over personen. Andere (commerciële) partijen hebben die belangstelling ook. De overheid kan echter invloed uitoefenen op de grenzen van het juridisch toelaatbare, bijvoorbeeld door te zorgen voor verantwoord gebruik van RFID. Het Rathenau Instituut organiseerde hierover onlangs een seminar. Overheid Innovatief doet verslag.

Technologische en wetenschappelijke ontwikkelingen gaan vaak erg snel. Het Rathenau Instituut stelt zich ten doel al in een vroeg stadium stil te staan bij maatschappelijke gevolgen van technologie en wetenschap. Men kijkt dan naar zaken als wenselijkheid, veiligheid en verantwoordelijkheid. De snelle introductie van *RFID tags* is zo'n technische ontwikkeling die tot de verbeelding

Wat kunnen en mogen opsporingsdiensten met digitale voetsporen doen?

spreekt. Bij het seminar - in de Haagse, prestigieuze Sociëteit De Witte - spraken diverse vertegenwoordigers van belangenorganisaties, het bedrijfsleven én Kamerleden over de mogelijkheden en onmogelijkheden van *RFID als opsporingsmiddel*. Zo stipte de voorzitter van het College van Procureurs-generaal Harm Brouwer aan wat de onstuitbare opkomst van RFID nu voor het openbaar ministerie betekent. Hij focuste daarbij op de strafrechtelijke handhaving van de rechtsorde. De kortgeleden gepromoveerde Bart Schermer van ECP.NL/RFID Platform Nederland, prikkelde de toehoorders met de uitspraak, dat er over twintig jaar geen privacy meer bestaat. Het programma ging echter van start met een lezing van Christian van 't Hof over het gebruik van RFID in het dagelijkse leven. In een afsluitende paneldiscussie kruisten aanwezigen in de zaal de degens met VVD-, CDA-, PvdA en SP-Kamerleden, als ook met Madeleine McLaggan-Van Roon (College Bescherming Persoonsgegevens) en Jeroen Terstegge (Privacy Officer bij Philips en lid van de Privacywerkgroep VNO-NCW).

Voetsporen

RFID staat voor Radio Frequency IDentification. De techniek wordt tot nu toe vooral toegepast in de logistiek om goederen te identificeren, maar neemt steeds meer bezit van het publieke domein. De bekendste voorbeelden zijn de OV-chipkaart, het biometrische paspoort en toegangssystemen op kantoren. RFID dient dan vooral als elektronische sleutel of portemonnee. Omdat RFID-systemen net zoals internet en telefoonverkeer 'digitale voetsporen' achterlaten, zijn er veel meer mogelijkheden. Vooral als het gaat om het opsporen van verdachten of getuigen. RFID wordt hierdoor steeds interessanter voor opsporingsdoeleinden. De vraag is echter 'wat kunnen en mogen opsporingsdiensten met digitale voetsporen - technisch en juridisch gezien - doen?' Is het wenselijk om

Hoe werkt RFID?

Een RFID systeem bestaat uit RFID-chips, chipslezers, een netwerk en een database die informatie uitwisselen. Als de chip dicht genoeg bij een chiplezer komt, geeft die zijn code af. De code gaat via het netwerk naar de database, waar hij wordt geïdentificeerd, bijvoorbeeld als een bepaald product of persoon. Aanvullende informatie kan vervolgens worden teruggestuurd naar de plek waar de chip werd uitgelezen, waarna een reactie volgt (bijv. prijsberekening of opening van een deur). Die handelingen worden dan meestal weer geregistreerd, zodat het netwerk kan bijhouden waar en wanneer, welke chip tot welke actie leidde. RFID is meer dan een barcode. RFID-chips kunnen veel meer informatie bevatten, sneller - in grote groepen en onzichtbaar - worden uitgelezen en in sommige gevallen kan de *tag*-informatie worden aangepast. Betalen aan de pomp kan bij Shell met de Easypay RFID-chip. Voetbalstadia gaan steeds meer over op een RFID-clubkaart als toegangssysteem. Menig kantoor heeft trouwens zo'n toegangssysteem.

deze mogelijkheden ook daadwerkelijk te benutten. Brouwer onderscheidt drie terreinen waarop RFID's voor het OM relevant zijn. Dat zijn respectievelijk de informatievergaring voor de opsporing, de bescherming van de persoonlijke levenssfeer van burgers, en RFID-gerelateerde vormen van criminaliteit. Dieven die met een *tag*-lezer straten afstruinen op zoek naar waardevolle spullen, vreest hij minder. Een serieuzer risico vormt de crimineel die er in slaagt een RFID uit te schakelen of te kopiëren. Hij kan dan eenvoudig toegang krijgen tot vertrouwelijke gegevens en goederen, of zich andermans identiteit aanmeten. Informatiegaring met behulp van RFID's is in beginsel gunstig voor de opsporing van strafbare feiten.

1.000 miljard tags

Brouwer weerlegt de beschuldiging van gespreksdeelnemers dat het OM telkens om nieuwe bevoegdheden roept. "Voor zover ik nu kan overzien, biedt de huidige wetgeving over strafvorderlijke gegevensvergaring voldoende mogelijkheden om, wanneer dat noodzakelijk is voor de opsporing, RFID-informatie op te vragen." Het belangrijkste is volgens hem, de materiële afweging of het opvragen van gegevens aan de eisen van proportionaliteit en subsidiariteit voldoet. Die afweging vraagt terughoudendheid. Het uitgangspunt is immers 'nee, tenzij'. Wat privacy en de bescherming ervan betreffen, beklemtoont hij dat 'het OM de persoonlijke levenssfeer zonder meer het beschermen waard acht'.

Het betoog van Schermer handelt over klassieke en moderne opsporingsmethoden. Sherlock Holmes versus George Orwell, inclusief camerabewaking en databases van werkgevers, belastingdienst, ziektekostenverzekeraars, NS, enzovoort. Alles komt samen in de database van de Nationaal Coördinator Terrorismebestrijding (NCTb). In 2006 waren er 6 miljard *tags*, in 2020 zijn dat er 1.000 miljard, zo is de verwachting. RFID geeft meer controle over de publieke ruimte. Schermer: "Over twintig jaar bestaat er geen privacy meer. RFID is daar niet de oorzaak van, maar het vormt een onderdeel van een bredere ontwikkeling. Juridische en politieke keuzes beïnvloeden niet alleen de privacy en vrijheid, maar ook het gebruik en acceptatie van RFID." □

Illustratie Hans van den Tillaart

Big Brother

De mogelijkheden om mensen te volgen zijn in de praktijk nog begrensd. Afzonderlijke systemen geven nu slechts een beperkt beeld van de gebruikers. Dit kan echter veranderen, vrezen RFID-tegenstanders. Straks werken bijna alle toegangssystemen met RFID en kunnen andere technologieën eraan worden gekoppeld. Gebruikers laten steeds meer digitale voetstappen na en worden transparanter voor beheerders van die omgevingen. Omgekeerd worden de RFID-omgevingen voor gebruikers juist minder inzichtelijk. De huidige balans tussen keuze, gemak en controle kan dan verstoord raken. Dat heeft ook gevolgen voor de rol van de overheid. Enerzijds wordt het lastiger de Wet bescherming persoongegevens te handhaven. Anderzijds zal de overheid zelf meer gebruik kunnen maken van digitale voetsporen, bijvoorbeeld bij de opsporing van verdachten of getuigen.

Spelregels

'RFID is nooit een *plug and play* oplossing', aldus Sander de Ridder, directeur van CaptureTech, een specialist in automatische identificatie. Volgens hem is door de afwijkende eigenschappen van toe te passen frequenties het functioneren van een RFID-oplossing alleen maar te garanderen, door een loepzuivere afstemming van product, omgevingsfactoren en hoger gelegen systemen. In die systemen zijn door RFID-infrastructuur, chips en software alle procedures voor privacy verankerd. Als voorbeeld noemt hij het project bij Boekhandels Groep Nederland (BGN). "Het boek dat de koper van de plank haalt, wordt meteen herkend. Maar", zo voegt hij ter geruststelling toe, "wat met die informatie mag worden gedaan, is haarscherp vastgelegd in de spelregels van de detailhandel."