Inleiding

Zwenne, G.J.; Zwenne G.J., Schermer B.W.

1 Inleiding

Gerrit-Jan Zwenne

RFID is niet nieuw. Weliswaar kent minder dan één op de tien Nederlanders de term, maar toch maakt vrijwel iedereen er dagelijks gebruik van en zonder daar erg van onder de indruk te zijn. Op het werk kent iedereen de contactloze toegangspasjes, autosleutels openen en sluiten autodeuren van vijfentwintig meter afstand. Op buitenlandse snelwegen zien wij de tolpoortjes die auto's uitgerust met transponders automatisch registreren als deze langsrijden. Van een contactloze ski-pas of een geavanceerd toegangskaartje voor een voetbalwedstrijd kijkt niemand echt op. En hardlopers zijn bekend met de 'championchip', een plastic ding dat op de schoenen wordt bevestigd en feilloos vastlegt hoe snel er is gelopen over een hele of halve marathon.

Het zijn allemaal vertrouwde RFID-toepassingen waarbij niemand zich direct zorgen maakt over zijn of haar privacy of andere rechtsvragen. Waarom dan dit boekje? En waarom nu? Omdat er geen twijfel over is dat nagenoeg iedereen binnenkort te maken krijgt met meer en geavanceerdere identificerende draadloze chipjes, soms niet groter dan een rijstkorrel, waarvan de kosten minder dan een eurodubbeltje zijn en die dus op een ongekend grote schaal gaan worden toegepast. En zoveel lijkt wel zeker dat dat gaat worden gedaan op een manier waarvan wij niet altijd weten wat wij ervan moeten vinden. Een geruchtmakend, ook in dit boekje aangehaald voorbeeld betreft de chip die de vaste klanten van een Rotterdamse uitgaansgelegenheid onderhuids in hun bovenarm laten implementeren om gemakkelijk toegang te krijgen en drankjes af te rekenen. Daarover was indertijd nodige ophef – waarschijnlijk was het de betreffende club daar ook om te doen – en in nagenoeg alle commentaren werd gewezen op privacyrisico's en ook wel de lichamelijke integriteit of 'ontmenselijking'.[1] Het is tot daaraan toe dat chips bij koeien en paarden of honden en katten worden geïmplementeerd, als dat bij mensen gebeurt worden er grenzen overschreden die misschien niet zouden mogen worden overschreden. En zoals zo vaak wordt dan bijna automatisch geroepen om nieuwe en specifieke wet- en regelgeving.[2]

---

1 Vergelijk R. Foroohar, 'The Future of Shopping', *Newsweek* June 7-14: '…tiny silicon identity chips being put in everyday objects and even implanted under the skin are changing the way we consume; will they also invade our privacy?'

2 Vergelijk ChristenUnie, RFID-Chips, kans of gevaar?, (mei 2005).

Zo een reactie is voorspelbaar en begrijpelijk maar daarmee niet altijd de meest zinvolle. Dit boekje probeert een aanzet te geven voor een discussie over deze en andere RFID-toepassingen en de rechtsvragen waartoe die aanleiding geeft. In de eerste twee bijdragen wordt daartoe eerst in kaart gebracht wat RFID eigenlijk is, en wat er mee kan, nu en in de nabije toekomst. Bart Schermer bespreekt welke technologie, welke radiofrequenties en welke standaarden worden gebruikt. Vervolgens gaat Jeroen Terstegge in op verschillende toepassingen, uiteenlopend van elektronische autosleutels, bankpassen en paspoortbeveiliging tot het openbaarvervoerkaarten, tracking 'n tracing van postpakketten en vrachtcontainers, schroeven, moeren en bouten. Zijn conclusie is dat deze technologie uiteindelijk niet meer goed valt te brengen onder de reikwijdte van de bestaande privacywetgeving. Dat betekent volgens hem het einde van de privacywetgeving zoals wij die nu kennen. Om dat probleem op te lossen doet hij de suggestie om uit te gaan van privacy-by-design: niet pas bij de toepassing van de technologie nadenken over een zorgvuldig gebruik, maar al bij de ontwikkeling ervan. Dat ligt inderdaad voor de hand. De wijze waarop informatiesystemen en -infrastructuren worden opgetuigd is bepalend voor de regulering van het gebruik ervan.[3] En dat is voor RFID niet anders. Omdat maar weinigen ervoor zullen kunnen kiezen om er geen gebruik van te maken, is het essentieel dat er vooraf is nagedacht over afdoende privacy- en andere waarborgen.

In de andere bijdragen in dit boekje brengen de auteurs in kaart wat de huidige wetgeving betekent voor RFID. Het gaat hier om de wettelijke grenzen die er op dit moment zijn. Peter Blok geeft in dat kader een overzicht van de belangrijkste elementen van de privacywet, de Wet bescherming persoonsgegevens. Om aan de werking van deze wet te ontkomen geeft hij in overweging om de technologie alleen te gebruiken om anonieme gegevens te verzamelen. Ook hij denkt dus aan oplossingen in de sfeer van privacy-by-design. De toepassing van RFID in de zorg wordt besproken in de bijdrage van Roel Croes. Dit is, zo blijkt uit zijn overzicht, een omvangrijk toepassingsgebied en er zijn dan ook talloze nog onbeantwoorde vragen. In andere verhoudingen, namelijk die tussen werkgever en werknemer ligt het voor de hand dat RFID een rol zal spelen in personeelvolgsystemen. Jessica Verwer gaat hier in haar bijdrage op in. Zij raadt werkgevers aan gedragscodes voor personeelvolgsystemen op te stellen vergelijkbaar met de gedragscodes die wel worden gebruikt voor de controle op het e-mail- en internetgebruik van werknemers.

---

3 L. Lessig, (1999), *Code and other Laws of Cyberspace*, New York: Basic Books.

De vraag in hoeverre misbruik van RFID-systemen kan worden gebracht onder de thans geldende strafbepalingen, wordt beantwoord in nog een bijdrage van Bart Schermer. Hij zoekt daarbij vooral aansluiting bij de bepalingen over computercriminaliteit en ook wel bij die over heimelijk cameratoezicht. Hij stelt vast dat het afluisteren van onbeveiligde RFID-signalen niet strafbaar is. Hoewel daar wel wat voor te zeggen is – dan moet de toepasser maar zorgen voor adequate beveiliging – is het wel de vraag wat je als gebruiker daaraan hebt. Als wordt gekozen voor goedkope maar afluisterbare chips hebben consumenten, werknemers en reizigers daar in de eerste plaats last van, niet (of in veel mindere mate) het warenhuis, de werkgever of het busbedrijf. Een autofabrikant begrijpt wellicht dat een adequate beveiliging van de draadloze autosleutel ook in zijn belang is – een auto zonder goed slot is onverkoopbaar. Maar de vraag is of dat ook zonder meer geldt voor andere toepassers van de RFID. Het is niet vanzelfsprekend dat producenten, toepassers en gebruikers dezelfde perceptie hebben van een afdoende waarborgen. Voor wet- en regelgeving die uitgaat van privacy-by-design is van belang dat daarover wel overeenstemming is.

Jeroen Koëter, ten slotte, geeft een overzicht van wetgevings- en zelfreguleringsinitiatieven in het buitenland. Interessant zijn natuurlijk de ontwikkelingen in de landen waar RFID al op grote schaal wordt toegepast, te weten Japan en – in mindere mate – de VS. Ook wijst hij erop dat in sommige landen bewust is gekozen om RFID (nog?) niet door middel van specifieke wetgeving te reguleren.

Daarmee is dit boekje niet volledig. Het bespreekt maar een paar rechtsverhoudingen en dat dan op verkennende wijze. Er zijn allerlei andere rechtsverhoudingen waarin de implicaties van RFID minstens zo ingrijpend zijn. Eén daarvan is de verhouding van reiziger en openbaarvervoerders. Met de OV-chipkaart wordt RFID ook daar toegepast en ook dan zijn er vragen over de bescherming van de privacy van de reizigers. Op dit moment laat het zich aanzien dat de meest gebruiksvriendelijke en goedkoopste varianten van de chipkaart met behulp van RFID worden geoptimaliseerd om zoveel mogelijk reisgegevens van identificeerbare reizigers vast te leggen. Wie dat niet wil kan kiezen voor een geanonimiseerde chipkaart, maar het gebruik daarvan wordt niet door de openbaarvervoerbedrijven aangemoedigd. Onduidelijk is nog of abonnements- en kortingskaarthouders gebruik kunnen maken van een kaart waarmee alleen de gegevens worden vastgelegd, die nodig zijn voor de betaling van de gemaakte reizen – van jaarkaarthouders zouden dan géén identificeerbare reisgegevens hoeven te worden vastgelegd omdat deze gegevens niet relevant zijn voor de betaling.

Het lijkt er dus op dat veel reizigers na de invoering van de OV-chipkaart niet meer gebruik kunnen maken van het openbaar vervoer zonder dat hun reisgegevens voortdurend worden vastgelegd. Dat is niet niks. RFID maakt het reizen gemakkelijker en misschien ook wel veiliger. Maar dat maakt het nog niet vanzelfsprekend dat er reisgegevens worden verzameld voor marketing en andere doeleinden. Daarover is nog weinig discussie. Of dat betekent dat reizigers zich wel kunnen vinden in de OV-chipkaart, is iets dat nog zal moeten blijken. Veel zal afhangen van de wijze waarop de openbaarvervoersbedrijven kunnen uitleggen waarvoor ze de reisgegevens nodig hebben en wat zij ermee gaan doen.

Alle bijdragen in dit boekje zijn geschreven op persoonlijke titel.