Privacy en andere juridische aspecten van RFID:
unieke identificatie op afstand van producten en personen

Privacy en andere juridische aspecten van RFID: unieke identificatie op afstand van producten en personen

Studiecommissie RFID

Redactie
Gerrit-Jan Zwenne & Bart Schermer

Nederlandse Vereniging voor Informatietechnologie en Recht (NVvIR)

Privacy en andere juridische aspecten van RFID:
unieke identificatie op afstand van producten en personen
ISBN 90 5901 722 6
NUR 820

Inhoud

Voorwoord

Een bescheiden fabriekshal. Dat was de ruimte om een willekeurige computer in 1965 neer te zetten. In datzelfde jaar publiceerde Gordon Moore het vermoeden dat de ruimte die nodig is voor elektronische componenten elk jaar halveert. De wet van Moore is veertig jaar oud en geldt nog steeds. We leven nu dan ook in een tijd die het toestaat minuscule computertjes op voorwerpen te plakken en in levende wezens te injecteren. En er zijn tekenen die aangeven dat deze wet nog zeker tien jaar zal meegaan. Wat dat betekent voor RFID-tags tart ons voorstellingsvermogen.
Een systeembeheerder. Die hadden we in 1985 nodig om programmatuur op computers te installeren, te configureren en te onderhouden. We maakten ons toen zorgen over de mate, waarin we ons van systeembeheer afhankelijk maakten en wat die allemaal niet van ons wisten. Bovens bedacht het begrip 'system-level bureaucratie,' en de system-level bureaucraten bedachten het begrip 'trusted computing'. Inmiddels is het gemeen goed geworden om de diensten die we op onze PC's gebruiken online te verbinden met de dienstverlener, die volautomatisch verbeteringen en veranderingen aanbrengt en vaak registreert wat we doen. Wat dat betekent voor de gegevensverzamelingen die over ons rondzwerven, tart ons voorstellingsvermogen.
Het einde van het maakbaarheidsdenken. Dat was de belangrijkste collectieve conclusie van de politieke wetenschap sinds de jaren tachtig van de vorige eeuw. Ik vraag mij af, of dat inzicht is doorgedrongen tot de hedendaagse system-level bureaucraten van Microsoft, van Google en van de EU, met zijn bewaarplicht voor verkeersgegevens. Ik vrees dat het implanteren van administratie-op-afstand functionaliteit in computerdiensten en objecten zal blijven groeien, omgekeerd evenredig met de wet van Moore. Na Internet en de mobiele telefonie is er nu de RFID. Wat dat betekent voor onze autonomie tart ons voorstellingsvermogen.

Wat dit alles betekent voor ons rechtssysteem eveneens. Ik heb dan ook nooit goed kunnen begrijpen waarom wetenschapsbestuurders wél investeren in de innovatie van techniek en niét in onderzoek naar de duurzaamheid van ons recht. Het boek dat voor u ligt is geschreven door een studiecommissie van de Neder-

landse Vereniging voor Informatietechnologie en Recht, een collectief dat zich wél verantwoordelijk voelt. Ik beveel het u aan.

Prof. mr. Aernout H.J. Schmidt
eLaw@Leiden
Centrum voor Recht in de Informatiemaatschappij
Universiteit Leiden

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.

2 Wat is RFID?[4]

Bart Schermer

Om een correct inzicht te krijgen in de juridische (meer in het bijzonder privacyrechtelijke) aspecten van RFID is het noodzakelijk een goed begrip te hebben van de technologie. In dit hoofdstuk zal een beeld worden geschetst van RFID-technologie, de toepassingen en de verwachtingen voor de toekomst. Speciale aandacht zal worden besteed aan de technische werking van RFID-systemen. De reden hiervoor is dat de werking van de techniek uiteindelijk bepaalt welke juridische aspecten relevant zijn. Voorts zullen enkele praktijkvoorbeelden worden gegeven van RFID-systemen opdat een beter beeld gevormd kan worden van hoe RFID binnen onze maatschappij toegepast wordt en gaat worden.

2.1 Definitie RFID

RFID staat voor Radio Frequency Identification[5] en is een technologie waarmee met behulp van radiosignalen de unieke identificatie van producten, dieren en personen op afstand mogelijk wordt gemaakt. Zoals de naam aangeeft is de primaire functie van RFID automatische identificatie met behulp van radiofrequentie(RF-)technologie.

2.1.1 Automatische identificatie

Automatische identificatie en data capture (AIDC) is een verzamelnaam voor apparatuur en programmatuur die het mogelijk maakt om snel en accuraat informatie over objecten, mensen of dieren te verzamelen, op te slaan en te raadplegen. Wanneer gebruik wordt gemaakt van AIDC-technologie is het niet langer noodzakelijk om handmatig informatie in te voeren in een geautomatiseerd systeem. Veruit de bekendste vorm van AIDC is de streepjescode (barcode). Wanneer een barcode wordt uitgelezen dan wordt de informatie uit de streepjescode (meestal een nummer) automatisch ingelezen in bijvoorbeeld een kassa- of voorraadsysteem. Bij AIDC kan de opslag en overdracht van informatie op verschil-

[4] Delen van dit hoofdstuk zijn eerder verschenen in een publicatie privacyrechtelijke aspecten van RFID van ECP.NL (www.ecp.nl).

[5] Een lijst met alle in dit boek gebruikte afkortingen is achterin opgenomen.

lende manieren plaatsvinden, bijvoorbeeld door gebruik te maken van magneetkaarten of barcodes. Bij RFID wordt de informatie draadloos overgebracht met behulp van radiogolven.

2.1.2 RF-technologie

Radiogolven (energie in de vorm van elektromagnetische trillingen) kunnen gebruikt worden om informatie draadloos over te brengen tussen twee punten. Het bekendste voorbeeld van deze technologie is de AM/FM-radio, maar andere toepassingen die gebruikmaken van radiogolven, zoals de mobiele telefoon en draadloze netwerken, zijn ook niet meer weg te denken uit ons dagelijks leven.

Radiogolven hebben een bepaalde frequentie. Het elektromagnetisch spectrum kent verschillende frequenties van laag tot extreem hoog. Omdat grote delen van dit spectrum al worden gebruikt voor andere toepassingen zoals bijvoorbeeld AM/FM-radio, is niet elke frequentie beschikbaar voor RFID. De voor RFID gangbare frequenties variëren van laag frequent tot zeer hoog frequent en zijn: 125KHz (LF),13.56MHz (HF), 860 tot 950 MHz (UHF), en 2.45GHz (microwave).[6]

Het gebruik van verschillende frequenties is noodzakelijk omdat iedere frequentie anders reageert op de fysieke wereld. Omdat radiogolven over het algemeen moeite hebben om door metalen objecten of vloeistoffen heen te dringen, zijn metalen objecten en objecten met een hoog vloeistofgehalte (bijvoorbeeld fruit en dranken) moeilijker te identificeren met behulp van RFID. Lage frequenties zijn het beste geschikt om door vloeistof en metaal heen te dringen. Hier staat tegenover dat de maximale leesafstand niet erg groot is en de snelheid waarmee data overgedragen kan worden laag is. Ultra High Frequency (UHF) heeft een grotere maximale leesafstand en hogere datatransmissie snelheid, maar is duurder, consumeert meer stroom en heeft meer moeite om door vloeistoffen en metalen te dringen. De keuze voor de technische inrichting van een RFID-systeem is dus in belangrijke mate afhankelijk van de gekozen toepassing en de bijbehorende kosten.

---

6 LF staat voor low frequency, HF voor high frequency, en UHF voor ultra high frequency.

2.2 De opbouw van een RFID-systeem

Kort gezegd werkt RFID als volgt: een chipje gekoppeld aan een antenne kan radiosignalen opvangen die worden uitgezonden door speciale leesapparaten. Het chipje gebruikt de elektromagnetische energie van het uitgezonden radiosignaal om een bericht terug te sturen aan het leesapparaat. De inhoud van dit bericht is de informatie die opgeslagen ligt in de chip. Meestal zal dit slechts een uniek nummer zijn, maar er kan ook aanvullende informatie in de chip worden opgeslagen zoals productinformatie.

Een RFID-systeem bestaat over het algemeen uit drie onderdelen:
– de RFID-*tag*;
– de RFID-*reader*; en
– een *middleware* oplossing (een systeem om RFID-data te verwerken).

2.2.1 Tags

Een RFID-radio-etiket (tag of transponder) is het onderdeel van een RFID-systeem dat wordt bevestigd op het te identificeren object. Een tag bestaat uit een aantal onderdelen te weten: een chip, een antenne en een omhulsel.
– *Chip*. De chip is een halfgeleider die informatie over, of een verwijzing naar, het object waar het aan gehecht is in zich draagt. De hoeveelheid en het type informatie dat vastgelegd kan worden in de chip is afhankelijk van het gekozen dataformaat en de beschikbare geheugencapaciteit. De chip kan read only zijn, wat betekent dat data op de chip enkel is uit te lezen en niet is aan te passen, write once waarbij de chip maar één keer beschreven kan worden of read-write, wat betekent dat de chip uitgelezen kan worden maar dat ook informatie toegevoegd of verwijderd kan worden.
– *Antenne*. De antenne die aan de chip vastzit zendt, afhankelijk van het type tag, zelf radiogolven uit of gebruikt de energie van de ontvangen radiogolven om een signaal terug te zenden.
– *Omhulsel*. Om de chip en de antenne te beschermen en bevestiging op en in objecten mogelijk te maken, worden tag en antenne in een omhulsel gegoten.

Chip, antenne en omhulsel vormen samen de RFID-tag. Er zijn verschillende typen tags:
– *Actieve tag*. Een actieve tag bevat naast een chip en antenne ook een eigen krachtbron in de vorm van een batterij. Door de eigen krachtbron is de tag in staat om een zwakker radiosignaal te ontvangen en het antwoord uit te zenden

over een grotere afstand. Hier staat tegenover dat de levensduur door de batterij beperkt is en de tag over het algemeen groter en tevens duurder is.
– *Passieve tag*. Een passieve tag heeft geen eigen batterij hetgeen betekent dat de tag energie moet ontvangen van het radiosignaal van de reader. De tag verkeert dus in een 'slaaptoestand' totdat deze een radiosignaal van een reader opvangt. Voordeel van passieve tags is dat ze relatief goedkoop zijn en door het ontbreken van een eigen batterij klein gehouden kunnen worden. Passieve tags zijn daarom bij uitstek geschikt om individuele producten van RFID te voorzien (item level tagging). Doordat de tag geen eigen krachtbron heeft is de maximale leesafstand van de tag beperkt tot ongeveer vijf meter.
– *Semi-passieve tag*. Een semi-passieve tag heeft een eigen batterij welke niet wordt gebruikt om de leesafstand te vergroten, maar om de intelligentie en de geheugenopslagcapaciteit van de chip te verbeteren.

2.2.2 Readers

Een reader (lezer of interrogator) is het apparaat dat tags kan uitlezen. De reader doet dit door het uitzenden van een radiosignaal waarop RFID-tags die zich binnen het bereik van het signaal bevinden kunnen reageren. Een reader bestaat uit een antenne en een controle-eenheid. De controle-eenheid codeert, decodeert, controleert en bewaart RFID-data en zorgt voor de communicatie met de tags en eventueel een achterliggend databasesysteem.[7] De readers kunnen zowel vast (bijvoorbeeld boven een deur of in een schap) als mobiel zijn (handhelds, PDA's et cetera).

Zoals reeds eerder vermeld, wordt de maximale leesafstand van een reader en de bijbehorende tags bepaald door de gebruikte frequentie van het radiosignaal. Zo kan een UHF-reader de bijbehorende UHF-tags van grotere afstand lezen dan een laagbandige reader dat kan bij RFID-tags die gebruikmaken van lage frequenties. Een andere factor die de leesafstand beïnvloedt is het vermogen (in Watt) van de reader. Een hoger vermogen betekent een grotere leesafstand.

2.2.3 RFID middleware-oplossingen

Middleware-oplossingen zorgen voor de koppeling van RFID-data met de achterliggende ICT-infrastructuur van de gebruiker. RFID-readers die tags lezen gene-

7 IBM, (2003), *Global Commerce Initiative EPC Roadmap*, p. 11.

reren al snel een enorme hoeveelheid data en hoewel de eerste filtering en verwerking reeds in de reader plaatsvindt, is een verdere bewerkingsslag vaak noodzakelijk. De data uit de reader wordt daartoe door een middleware-oplossing verwerkt en doorgestuurd om vervolgens gebruikt te kunnen worden in andere ICT-infrastructuren van de organisatie zoals bijvoorbeeld ERP- of CRM-systemen.

2.3 Het EPC Global Network[8]

Het EPCglobal Network is een door EAN en het Uniform Code Council (UCC)[9] binnen het Auto-ID lab ontwikkelde set van standaarden voor onder meer het vastleggen van unieke nummers in RFID-tags binnen de logistieke keten. Deze nummers kunnen gekoppeld worden aan databases waarin eveneens gestandaardiseerde informatie is vastgelegd over het product. Hiermee wordt het mogelijk om individuele producten te identificeren en bijbehorende informatie over deze producten op te zoeken. Gezien het belang van het EPCglobal Network en het feit dat de discussie rondom RFID en privacy zich momenteel grotendeels toespitst op het gebruik van RFID in consumentengoederen, zal nadere aandacht worden besteed aan dit initiatief. De standaardisatiewerkzaamheden rondom het EPCglobal Network dienen echter in breder verband te worden gezien. Zo zullen de EPCglobal standaarden bijvoorbeeld in ISO- en CEN-normen geïncorporeerd worden. Daarnaast zijn er nog tal van gebieden waar RFID gebruikt wordt maar waarop het EPCglobal Network niet ziet (bijvoorbeeld de identificatie van personen). Ook op deze gebieden wordt gewerkt aan internationale standaarden.
De technische en organisatorische werking van het EPCglobal Network is nog niet volledig uitgekristalliseerd. Hierdoor blijft een verkenning van het EPCglobal Network (ook in juridische zin) tot op zekere hoogte tentatief.

2.3.1 Electronic Product Code (EPC)

Aan de basis van het EPCglobal Network ligt de Electronic Product Code. Electronic Product Code, afgekort EPC, is de nummerstandaard die voor de identificatie van objecten wordt gebruikt. De huidige EAN.UCC nummerstandaard wordt gebruikt in het EPCglobal Network. De EPC is een (vooralsnog 96 bits) code die de fabrikant, de productcategorie en het itemnummer van een artikel

---

8 Zie ook de bijdrage van Jeroen Terstegge.

9 De beide organisaties gaan sinds februari 2005 verder onder de naam GS1 (zie: <http://www.gs1.org>)

aangeeft. Het Auto ID Center heeft een 64-bitsversie en een 96-bitsversie van de code voorgesteld. Versies met meer bits worden voorlopig niet toegepast omdat het extra geheugen de chip (en daarmee de tag) duurder maken. Op de chip zelf wordt enkel de EPC vastgelegd, geen additionele informatie. Omdat binnen het EPCglobal Network de EPC te koppelen is aan informatie in een achterliggende database, is het niet noodzakelijk om alle informatie op te slaan op de chip zelf, hetgeen kostenbesparend werkt. De tag is standaard *niet* voorzien van encryptie.

2.3.2 Middleware

De koppeling tussen readers en achterliggende applicaties (zoals voorraadbeheer) geschiedt via middleware-oplossingen. In de oorspronkelijke opzet van het systeem werd dit deel van het EPCglobal Network de 'Savant' genoemd. De middleware-oplossing wordt gevormd door gedistribueerde, hiërarchisch georganiseerde netwerkcomponenten welke de informatiestromen die worden gegenereerd door diverse readers aggregeren, organiseren en coördineren. Met behulp van middleware kan een lokaal netwerk van readers worden gecreëerd. De middleware-oplossing kan de (georganiseerde) informatie van diverse readers doorsturen naar een hiërarchisch hoger middleware-component van de middleware-oplossing. Op deze manier kan een robuust, decentraal georganiseerd netwerk worden gemaakt dat goed schaalbaar is en bestaande of publieke bedrijfsnetwerken niet overbelast met EPC-data.

2.3.3 Physical Markup Language (PML)

De Physical Markup Language (PML) is een op XML-gebaseerde vocabulaire om informatie over producten uitgerust met EPC-tags weer te geven en te distribueren. Het doel van de PML is om de interface tussen het EPCglobal Network (bijvoorbeeld de readers) en bestaande ERP- en SCM-systemen te standaardiseren, waardoor communicatie tussen deze verschillende systemen mogelijk wordt.[10]

2.3.4 Object Name Service (ONS)

Omdat op de tags binnen het EPCglobal Network alleen de EPC wordt opgeslagen en geen verdere informatie, is een systeem noodzakelijk dat de EPC koppelt aan informatie over het product. De Object Name Service (ONS) vervult deze

[10] www2.inf.ethz.ch/~floerkem

taak. Het ONS is een volledig geautomatiseerde adresseringsdienst welke qua werking te vergelijken is met het Domain Name System (DNS). De Object Name Service koppelt een EPC aan het IP-adres van een EPC-IS waarin meer informatie is te vinden over het product. Het beheer en de operatie van het ONS is door EPCglobal uitbesteed aan Verisign.

2.3.5 EPC-Information Service (EPC-IS)

De EPC-Information Services zijn de daadwerkelijke opslagplaatsen waar informatie over met een EPC geëtiketteerd object vastgelegd is. Een informatievragende partij kan middels de EPC-IS-informatie krijgen over een met een EPC geëtiketteerd product. Een EPC-IS bevat de voor het EPC-netwerk relevante gegevens van het object. Dit betreft een subset van de informatie die in een bedrijfsinterne applicatie is geregistreerd welke buiten de 'firewall' van het bedrijf aan het netwerk beschikbaar wordt gesteld. Zo'n EPC-IS kan bij het bedrijf zelf zijn opgesteld, maar ook bij een dienstverlener, die dan een EPC-Information Service aanbiedt.

2.3.6 EPC Discovery Services (EPC-DS)

De EPC Discovery Services maken het (in samenhang met de Object Name Service) mogelijk voor de betrokken partijen om binnen de logistieke keten meerdere gedistribueerde EPC Information Services aan te spreken. Dit betekent dat Bedrijf A informatie over een product kan opvragen welke ligt opgeslagen in de EPC-IS van bijvoorbeeld Bedrijf B en Bedrijf C. Een EPC-DS verschaft een verwijzingsmechanisme dat gebruikers in staat stelt om snel te achterhalen in welke EPC-IS'en informatie over de EPC te vinden valt. Een EPC-DS is dus als het ware een zoekmachine op het EPCglobal netwerk.

2.4 Toepassingen en verschijningsvormen

Omdat RFID een verzamelnaam is voor allerlei toepassingen van radio-identificatietechnologie worden verschillende soorten RFID-systemen veelal op één hoop gegooid. Met het oog op het bespreken van de juridische aspecten van RFID is het echter van belang onderscheid te maken tussen verschillende toepassingen, omdat de concrete toepassing (en de daarbij behorende technische inrichting) bepaalt welke juridische consequenties er al dan niet zijn.

De systemen die worden gebruikt voor radio-identificatie kunnen grofweg worden verdeeld in vier categorieën: *smart labels*, *tokens & smart cards*, *implantaten*, en *overige systemen*. Al naar gelang de concrete toepassing zal een van deze vier systemen worden gebruikt.

2.4.1 Smart labels

Smart labels zijn passieve tags die door hun geringe prijs en afmeting op allerlei producten kunnen worden bevestigd. Omdat smart labels zo goedkoop mogelijk gehouden moeten worden om het rendabel te houden producten van RFID te voorzien, zal de op een smart label vastgelegde informatie zich nagenoeg altijd beperken tot een uniek nummer. Dit nummer kan aan een achterliggende database met additionele informatie over het product worden gekoppeld. In feite is de veelgebruikte term smart label dus enigszins misleidend, omdat de smart label op zichzelf niet bijzonder intelligent is of veel data kan bevatten. In feite is een smart label een 'object tag', een RFID-tag die bedoeld is voor het registreren van objectgegevens en niet voor toepassingen op persoonsniveau.
Het gebruik van smart labels wordt voornamelijk binnen de logistiek en detailhandel (op de zogenaamde *fast moving consumer goods*) overwogen. Grote partijen als Wal*Mart en Tesco stimuleren actief het gebruik van RFID smart labels in de detailhandel.

Otto
De Otto Groep, het grootste postorder bedrijf ter wereld, ziet RFID als een belangrijk onderdeel van haar bedrijfsstrategie. Eind 2004 is in het disitributiecentrum in Hamburg op uitgebreide schaal geëxperimenteerd met RFID. Dure goederen zoals camera's en mobiele telefoons werden uitgerust met RFID-tags. Deze tags werden op twaalf verschillende punten uitgelezen. Op deze manier kon onder andere bepaald worden of orders juist gealloceerd werden en of producten per abuis of opzettelijk verdwenen uit de keten (shrinkage). Gezien de positieve resultaten van de proef overweegt Otto inmiddels om RFID volledig uit te rollen binnen de organisatie. Otto probeert nu ook haar toeleveranciers ervan te overtuigen om ook RFID te gaan gebruiken. Op deze manier kan de volledige logistieke keten van Otto met RFID worden uitgerust.

2.4.2 Tokens & smart cards

RFID kan ook gebruikt worden om bestaande identificatie-, authenticatie- en autorisatiemethoden te vergemakkelijken en beter te beveiligen. Het gebruik van tokens die helpen bij de identificatie, authenticatie en autorisatie van personen is wijdverbreid in onze maatschappij, denk bijvoorbeeld maar aan het gebruik van bankpassen en toegangskaarten. De gebruikte tokens worden steeds geavanceerder en intelligenter. De opkomst van zogenaamde 'smart cards' is hier het beste voorbeeld van. Smart cards zijn pasjes die een chip bevatten waarop (persoons)gegevens kunnen worden opgeslagen.
Vooralsnog dient in de meeste gevallen de smart card uitgelezen te worden met behulp van een smart card reader. Er bestaan echter ook contactloze smart cards die van een afstand uitgelezen kunnen worden. Het gaat hierbij niet om afstanden van meters, maar eerder van centimeters. Deze smart cards maken gebruik van RFID-technologie.
Naast contactloze smart cards bestaan er ook andere draagbare RFID-tokens, een voorbeeld hiervan is de RFID-armband die in Legoland wordt gebruikt om zoekgeraakte kinderen te localiseren.[11] Tokens hebben over het algemeen ook een beperkte leesafstand, maar RFID-tokens kunnen ook een actieve tag bevatten hetgeen de leesafstand aanzienlijk vergroot.

Academisch Ziekenhuis Akita
Het Academisch ziekenhuis van Akita (Japan) gebruikt RFID om te voorkomen dat patiënten de verkeerde medicatie toegediend krijgen. Patiënten, injectienaalden met medicatie en verplegend personeel krijgen allemaal een RFID-tag. Met behulp van een PDA kan gekeken worden of de combinatie patiënt-injectienaald klopt, waardoor de kans op het verkeerd toedienen van medicatie tot een minimum beperkt wordt. Ook kan met het systeem gezien worden wie van het verplegend personeel aan welke patiënt bepaalde medicatie heeft toegediend.

2.4.3 Implantaten

Het is ook mogelijk om RFID-tags in het menselijk lichaam te plaatsen. In de meeste gevallen zullen deze subdermale implantaten dezelfde functie vervullen als de hierboven genoemde tokens: zij vereenvoudigen het proces van identificatie, authenticatie en autorisatie. Uiteraard is een bijkomend voordeel dat de token niet verloren of gestolen kan worden, waardoor er een hoger beveiligingsniveau

[11] www.RFIDjournal.com

gerealiseerd wordt. Het gebruik van implantaten wordt wereldwijd voor diverse toepassingen overwogen, met name in de zorg.

Baja Beach Club
De eerste implantaten zijn in Nederland reeds ingebracht. De VIP-gasten van de Baja Beach Club in Rotterdam krijgen met een RFID-tag in hun arm automatisch gratis toegang tot de club, het VIP-deck en kunnen met behulp van hun tag ook de drank afrekenen.

2.4.4 Overige systemen

Naast deze drie redelijk uniforme systemen bestaat er nog een restcategorie waarin alle systemen vallen die niet onder de drie bovenstaande categorieën geschaard kunnen worden. Het gaat dan om zogenoemde maatwerksystemen waarbij de concreet toegepaste RFID-technologie afhankelijk is van de toepassing.

Het AMALFI Project
Het Franse kadaster in de regio's Bas-Rhin, Moselle and Haut-Rhin bestaat uit veertigduizend boeken verspreid over verschillende kantoren. Samen vormen deze boeken maar liefst tien kilometer archief. Doel is om dit hele archief te digitaliseren. Hiervoor moeten de boeken naar een speciaal bedrijf in de Elzas waar ze automatisch gedigitaliseerd kunnen worden. Maar omdat de informatie zo belangrijk en vertrouwelijk is moet aan de hoogste veiligheidsstandaarden worden voldaan. Ook mogen de boeken niet langer dan vijf dagen uit het archief verwijderd worden.
Om zowel veiligheid en snelheid te kunnen garanderen in het digitaliseringsproces wordt gebruikgemaakt van (onder andere) RFID-technologie. Ieder boek wordt uitgerust met een RFID-tag alvorens het het kadastergebouw verlaat in een speciale veiligheidscontainer. Door gebruik te maken van RFID kan tijdens elke stap in het proces het boek geïdentificeerd worden en is het boek altijd te volgen en te traceren. Het grote voordeel van RFID boven het gebruik van een barcode is dat het boek alleen de veiligheidscontainer hoeft te verlaten tijdens het digitaliseren, daar waar bij gebruik van een barcode het boek bij iedere stap in het transport handmatig gescand zou moeten worden. Dit laatste levert naast aanzienlijke vertraging ook een extra veiligheidsrisico op.

2.5 Wat nog meer?

In tegenstelling tot wat velen denken is RFID geen nieuwe technologie en wordt het reeds op grote schaal voor verschillende toepassingen gebruikt. Zo wordt RFID wereldwijd onder andere gebruikt voor toegangscontrole bij gebouwen, het identificeren van vee, anti-diefstalsystemen en het automatisch afrekenen van tol bij tolwegen.

Veel van de privacygerelateerde vragen bij het gebruik van RFID hebben betrekking op het gebruik van RFID in de detailhandel waar wordt gestreefd naar 'item level tagging'. De redenen waarom wij nog niet in het stadium van item level tagging zitten zijn hoofdzakelijk van technische en economische aard. Zo vormden de prijs, afmeting en gebrek aan standaardisatie van RFID-tags lange tijd een barrière voor een brede toepassing. Deze barrières worden echter in hoog tempo geslecht door de voortschrijdende stand van de technologie, miniaturisering, standaardisatie en massaproductie. De verwachting is dat binnen enkele jaren de prijs van RFID-tags dermate gedaald is, dat RFID-tags in of op elk product geplaatst kunnen worden. De schattingen wanneer item level tagging daadwerkelijk plaats gaat vinden lopen echter uiteen van 2007 tot 2015.
De penetratie van RFID op productniveau is hoofdzakelijk afhankelijk van de prijs van de individuele RFID-tag. Als het 'magische' prijskaartje voor een passieve RFID-tag wordt vijf dollarcent genoemd, pas bij deze prijs wordt item level tagging daadwerkelijk aantrekkelijk voor de meeste producten. Maar naast de prijs voor de RFID-tag zelf vormen ook de kosten voor de overige onderdelen van de EPCglobal Network-infrastructuur vooralsnog een barrière voor de uitgebreide toepassing van RFID. Tot die tijd zal RFID in de logistieke keten naar verwachting met name worden toegepast op returnable transport items (pallets, kratten, rolcontainers, trolleys) binnen een onderneming.

2.5.1 Ambient Intelligence[12]

Wanneer RFID in samenhang met andere technologieën (embedded systems, IPv6, kunstmatige intelligentie, robotica) op grote schaal in onze maatschappij toegepast gaat worden, dan zullen wij langzaam maar zeker een 'internet van dingen' creëren. Onder futuristen is de algemene consensus dat RFID één van de sleuteltechnologieën is die ons binnen enkele jaren het 'het internet van dingen' zal brengen. Het internet van dingen ligt zeker nog enkele jaren in de toekomst, maar de eerste stappen worden nu reeds gezet door de uitrol van RFID-technologie. Het internet van dingen hangt nauw samen met de concepten 'ambient intelligence' en 'ubiquitous computing'.
De visionaire computerdeskundige Mark Weiser beschreef in de jaren tachtig de verschillende stappen die het computertijdperk heeft doorgemaakt en nog door zal maken. Weiser verdeelt de ontwikkeling van het computertijdperk in de vol-

[12] Zie ook de bijdrage van Jeroen Terstegge.

gende drie fasen: het *mainframe* tijdperk, het tijdperk van de *personal computer* en het tijdperk van *ubiquitous computing* of *ambient intelligence*.[13]
De eerste stap in de ontwikkeling van het computertijdperk was het *mainframe*. Mainframes waren de allereerste computers, waarvan de ontwikkeling grofweg tijdens de Tweede Wereldoorlog begon. Deze allereerste computers waren geen 'desktop' of 'laptop' computers, maar enorm grote, dure en complexe machines. Mainframes namen al snel een volledige kamer of verdieping in beslag en dienden constant onderhouden te worden door een team computerexperts. Het spreekt vanzelf dat het draaiend houden van een mainframe een kostbare aangelegenheid was.
Omdat processorkracht in deze tijd een schaars goed was, moest de rekenkracht van de mainframecomputer verdeeld worden over vele gebruikers, het zogenaamde 'timesharing' concept. Het was niet ongebruikelijk dat wetenschappers in de rij stonden voor een mainframe computer met de rekenkracht van een moderne rekenmachine. Mainframes worden ook nu nog steeds gebruikt. Het gaat dan echter om zeer krachtige computers die door grote organisaties worden gebruikt voor kritieke applicaties zoals Enterprise Resource Planning.
De volgende stap in de ontwikkeling van het computertijdperk was de Personal Computer, oftewel de PC. Het goedkoper worden van microprocessoren en andere computeronderdelen, miniaturisatie, en de ontwikkeling van gebruiksvriendelijke interfaces, maakte het mogelijk om het mainframe terug te brengen tot een machine die op een bureau paste en dusdanig goedkoop dat een persoon een computer volledig voor zichzelf kon krijgen. Het PC-tijdperk is eind jaren zeventig ontstaan en we bevinden ons nu aan het eind van dit tijdperk.

Langzaam maar zeker begeven wij ons nu naar de derde fase in de ontwikkeling van het computertijdperk. In deze derde fase hoeven wij niet meer achter een computerscherm te zitten maar zullen steeds meer objecten zelf 'computers' bevatten. Door alledaagse objecten zoals koelkasten, koffiezetapparaten en lampen uit te rusten met een microprocessor kunnen wij onze leefomgeving steeds verder automatiseren. Hierdoor verdwijnt de computer steeds meer naar de achtergrond van ons leven, en wordt het als het ware een onzichtbaar instrument in ons dagelijks bestaan. Uiteindelijk zullen we op deze manier een volledig onzichtbare intelligente infrastructuur om ons heen creëren die alom aanwezig is. Dit is het idee achter 'ubiquitous computing' of 'ambient intelligence'.

---

13 Weiser, M., (1993), Some Computer Science Problems in Ubiquitous Computing, in: *Communications of the ACM*, juli 1993 en Weiser, M., (1993b), Hot Topics: Ubiquitous Computing, in: *IEEE Computer*, oktober 1993.

Om intelligente voorwerpen met elkaar en met mensen te laten communiceren moeten zij echter wel in verbinding met elkaar staan. Radiotechnologieën zoals WiFi, bluetooth, Zigbee, NFC en RFID maken het mogelijk dat apparaten en producten over korte afstand draadloos met elkaar kunnen communiceren. In feite ontstaat er door deze onderlinge verbondenheid van apparaten en producten een 'internet van dingen'.[14] Wij mensen kunnen via de bedieningspanelen van de diverse apparaten of via apparaten zoals de mobiele telefoon, de palmtop, tablet PC en laptop vervolgens opdrachten geven aan onze apparaten. Het is zelfs mogelijk dat apparaten deels hun taken zelf gaan uitvoeren omdat zij met behulp van kunstmatige intelligentie kunnen anticiperen op ons gedrag en onze voorkeuren begrijpen.
Vanuit het oogpunt van privacy heeft deze ontwikkeling als voornaamste consequentie dat de grens tussen de publieke sfeer en de private sfeer steeds moeilijker te trekken zal zijn. Jeroen Terstegge zal hier in zijn bijdrage nader op ingaan.

14 Meloan, S., (2003), *Toward a Global 'Internet of Things'*, Sun Microsystems.

3 Toepassingen en toekomst van RFID

Jeroen Terstegge

3.1 Inleiding

'RFID zal een grotere impact op onze samenleving hebben dan Internet heeft gehad'.[15] Dat lijkt nogal een boude uitspraak voor een bij de meeste mensen tot nog toe onbekende technologie.[16] Toch zal dit niet ver van de waarheid liggen. Zoals Kevin Ashton, medeoprichter van het Auto-ID center (de uitvinders van de RFID-chip met Electronic Product Code) zegt: 'We are entering the Sensor Age. In the 19th century machines could do, in the 20th century machines could think, but in the 21th century they will perceive'.[17] RFID-chips gecombineerd met sensortechnologie is daarvoor de key-technologie. Zogeheten '*adaptive spaces*' nemen onze aanwezigheid waar en stellen zich in op onze vooraf opgegeven voorkeuren. De '*Ambient World*' waarin wij door middel van convergentie van verschillende technologieën (onder andere mobiele telecom, wireless breedband internet, RFID, GPS, displays en sensor- en spraaktechnologie) en verschillende online-diensten op een natuurlijke wijze communiceren met de wereld om ons heen, wordt daardoor op afzienbare termijn een realiteit.

3.2 Typen RFID

'RFID' is een algemene term voor een verzameling van verschillende technologieën, die een aantal elementen gemeen hebben: ze bestaan uit een chip met een antenne, een leesapparaat, en sturen via een radiosignaal (RF) een unieke code uit (de 'ID'). RFID gebruikt de niet-gelicentieerde bandbreedtes in het radiospectrum, met name Low Frequency (LF) op 125-134.2 KHz, de High Frequency (HF) op 13,56 MHz, de Ultra High Frequency (UHF) op 865.5 – 867.6 MHz (Europa) en 915 Mhz (US), en de zogeheten 'Industrial, Scientific and Medical band' (ISM) op 2.4 GHz, ook wel de 'Super High Frequency' (SHF) of 'microwave-frequentie' genoemd omdat de magnetron ook die frequentie gebruikt. RFID-chips die in het

---

15 Aldus prof. Cor Molenaar, voorzitter van het RFID Platform Nederland op het 10e Nationale Privacycongres.

16 Volgens een onderzoek van CapGemini uit 2005 zou slechts 8% van de Nederlanders wel eens van RFID gehoord hebben.

17 Voorwoord bij Garfinkel & Rosenberg, (2005), *RFID, applications, security and privacy*, Addison-Wesley.

lage spectrum (LF en HF) opereren, gebruiken het zogeheten 'Near Field' van een radiogolf, waardoor korte (ca. 1 meter) tot zeer korte afstanden (< 10 cm voor contactloze smart cards) leesafstanden tussen de chip en het leesapparaat mogelijk zijn. Deze passieve chips (dus zonder batterij) worden '*close coupling RFID's*' of '*proximity* RFID's' genoemd, naar de wijze van energieoverdracht tussen chip en leesapparaat. Deze korte afstand alsmede de relatief lage snelheid van dit deel van het spectrum, bepaalt mede hun toepassingsmogelijkheden. De RFID-chips die daarentegen in het hogere deel van het spectrum opereren (UHF en ISM), gebruiken het 'Far Field' van de radiogolven en hebben daardoor grotere leesafstanden (maximaal 4 tot 6 meter[18] op UHF) en 1,5 meter op ISM. Passieve chips op deze frequenties communiceren met een leesapparaat door middel van zogeheten '*backscatter*' (een techniek vergelijkbaar met radar) en worden daarom ook wel *vicinity* RFID's genoemd. Deze frequenties hebben hogere snelheden waardoor zij met name geschikt zijn voor toepassingen waarin veel chips in korte tijd gescand moeten worden, zoals in het geval van supply chain management.

Overigens zijn er ook nog andere factoren die de keuze voor een specifieke chip in een bepaalde toepassing bepalen, zoals bijvoorbeeld de mate waarin de chip succesvol kan communiceren onder invloed van bepaalde omgevingsfactoren (water, metaal, glas) en natuurlijk de prijs, waarbij overigens moet worden opgemerkt dat er binnen een bepaalde frequentie door de technologieaanbieders weer verschillende soorten RFID-chips worden gemaakt. Zo zijn er voor de HF-band verschillende soorten RFID-chips beschikbaar, ieder met hun eigen eigenschappen. De belangrijkste onderverdeling op de HF-band is die tussen 'contactloze smartcards' en 'smart labels'. De smartcards hebben een leesafstand van maximaal 10 cm en hebben vanwege hun bedoelde toepassingsgebieden een aantal ingebouwde beveiligingen zoals chip/reader authenticatie, encryptie (3DES, AES, PKI) en password protectie voor toegang tot het geheugen. De contactloze smart card chip is dan ook behoorlijk prijzig, variërend van een paar dubbeltjes voor een wegwerp chip ('ultralight') voor losse kaartjes in het openbaar vervoer, tot een paar euro voor chips met standaardbeveiliging voor toegangspassen, en hele dure voor zwaar beveiligde paspoortchips. De smart tag op de HF-band daarentegen heeft een leesafstand van ongeveer 1 meter, heeft nauwelijks beveiligingen aan boord en is dus ook goedkoop (minder dan 50 eurocent *and dropping*).
In het schema hieronder kunt u zien hoe de verschillende typen RFID, hun eigenschappen en hun typische toepassingsgebieden met elkaar samenhangen. Let op:

[18] Dit zijn laboratoriumafstanden. In werkelijkheid wordt de leesafstand negatief beïnvloed door storende omgevingsfactoren zoals de aanwezigheid van water of metaal.

Binnen elk type zijn weer subtypes te onderscheiden, met in essentie dezelfde eigenschappen, maar geschikt voor andere specifieke toepassingen.

Band	**LF**	**HF**		**UHF**	**ISM**
type	Smart tag (HiTag)	Smart card (Mifare)	Smart tag (ICode)	Smart tag (UCode)	
ISO standaard	11784, 11785 14223, 18000-2	14443 18092 (NFC1) 21481 (NFC2)	15693 18000-3	18000-6 (UHF) 18000-4 (ISM) [EPC Class Gen 1 and Gen 2]	
EPC compliant	Nee	Nee	Ja	Ja	Ja
maximale leesafstand	1 meter	< 10 cm	1 meter	4 meter (Gen1) 6 meter (Gen2)	1,5 meter
encryptie	Ja (gematigd)	Ja (zwaar) 3DES, AES, PKI	Nee, maar mogelijk	Nee, maar mogelijk	
kill-feature	Nee	Nee	Ja (EPC) Ja/Nee (non-EPC)	Ja (EPC) Ja/Nee (non-EPC)	
leesomgeving	Water + Metaal +	Water +/– Metaal +/–	Water +/– Metaal +/–	Water – Metaal –	Water – – Metaal – –
typische toepassingsgebieden	– Animal ID – Ski ticketing – Elektronische sleutels – Tracking metalen objecten	– Openbaar vervoer – Paspoorten – Klantenkaarten – Bankpassen – Toegangsbadges – Werknemer ID – E-Purse	– Supply Chain Management – Eigendomsbeveiliging (EAS) – Container ID – Pallet- en krat tracking – Post- en pakketdiensten – Voorraadbeheer – Authenticatie van tickets voor evenementen – Anti-counterfeiting/Brand protection		

3.3 Elektronische sleutels

Er wordt tegenwoordig geen nieuwe auto meer verkocht zonder RFID-chip in de sleutel. Samen met een in de auto ingebouwd leesapparaat functioneert deze chip als een startonderbreker, en beveiligt de auto zo tegen diefstal. Soms wordt deze chip ook gebruikt om de autodeuren te ontgrendelen, maar in veel gevallen is dit nog steeds 'ouderwetse' infraroodtechnologie.
RFID kan ook gebruikt worden om deuren en poorten te openen door even met een pas langs een leesapparaat te zwaaien (dit zijn meestal op contactloze smart cards gebaseerde toegangscontrolesystemen) of als onderdeel van een zogeheten '*two-factor authenticatie*'-procedure om toegang te krijgen tot het bedrijfscomputernetwerk. Door het gebruik van radiogolven en wederzijdse card/reader-authenticatie hoeven werknemers vaak hun pas niet eens uit hun zak, tas of portemonnee te halen. Wel zullen ze vanwege de korte leesafstand van minder dan 10 centimeter hun pas, tas of portemonnee op het leesapparaat moeten leggen.

3.4 Animal ID

Een belangrijke toepassing van RFID-technologie is het 'taggen' van dieren. Rundvee, varkens, en andere dieren worden van een chip voorzien, zodat steeds de herkomst van het dier – en dus van het vlees – te herleiden is naar een specifieke boer of slachterij. Een continue herkomstbepaling van de dieren moet uitbraken van varkenspest en BSE in een vroeg stadium opsporen. Uiteindelijk zal deze informatie ook via RFID-chips op de verpakking van het vlees voor de consument beschikbaar zijn. RFID-technologie levert daarmee een serieuze bijdrage aan de voedselveiligheid. Verder wordt de RFID-chip gebruikt om te bepalen of een dier wel of geen eten krijgt uit de voederbak en om tellingen van de veestapel te doen.
RFID wordt ook toegepast bij huisdieren. Een glazen buisje met daarin een RFID-chip wordt bij het huisdier via een injectie in de nek ingebracht. Via een bijbehorend centraal registratiesysteem kunnen vermiste dieren hopelijk weer bij hun rechtmatige baasjes worden terugbezorgd.

3.5 Ticketing

Het toepassen van RFID-technologie in tickets geniet een steeds grotere belangstelling. Kaartjes voor het openbaar vervoer, sportevenementen (onder andere WK-voetbal, Olympische Spelen), popconcerten en andere massa-evenementen,

maar ook boarding-passen voor vliegtuigen worden van een RFID-chip voorzien. Door deze chips kan toegang worden verkregen tot diensten (bijvoorbeeld het openbaar vervoer), de echtheid van de kaartjes wordt gecheckt (sport- en evenementtickets), of kan de doorstroming van mensen worden vergemakkelijkt (stations, luchthavens, evenementen).
Een 'ticket' hoeft niet per se van papier te zijn. Met zogeheten *Near Field Communication*-technologie (NFC) kan een smart card in een mobiele telefoon of PDA als een tijdelijk of permanent elektronisch ticket fungeren. Simpelweg je telefoon tegen een leesapparaat aanhouden[19] is voldoende om de transactie tot stand te brengen en toegang te krijgen.

3.6 Openbare veiligheid/beveiliging

RFID zal steeds vaker worden toegepast in toepassingen om de openbare veiligheid te verhogen. Het afsluiten van perrons met elektronische toegangspoorten op trein- en metrostations is daarvan een voorbeeld. Maar ook de paspoortchip is bedoeld om de veiligheid te verhogen. In dat geval is het niet de chip zelf die deze functie vervult, maar zijn het de (biometrische) gegevens die in het geheugen van de chip zijn opgeslagen om persoonscontrole bij grensovergangen te verbeteren.
RFID-chips kunnen ook worden ingezet als beveiliging tegen diefstal in bijvoorbeeld winkels of musea. De zogeheten 'Electronic Article Surveillance'-functie (EAS) van de chips zorgt ervoor dat het alarm afgaat zodra een goed wordt meegenomen waarvan de chip niet is gedeactiveerd. Maar ook slimme schappen in de winkel kunnen pro-actief diefstal detecteren. Een slim schap registreert hoeveel producten nog in het schap staan (met als doel de beschikbaarheid van producten te verhogen). Een test van de Engelse supermarktketen Tesco en Gillette laat echter zien dat deze functie ook kan worden gebruikt om (vermoedelijke) diefstal waar te nemen. De achtergrond van de test was deze: scheermesjes behoren vanwege hun kleine omvang en hoge prijs tot de Top 3 van meest gestolen goederen in een supermarkt. De test hield in dat als een ongebruikelijke hoeveelheid scheermesjes, waarvan de verpakking door Gillette van een RFID-chip was voorzien, vrijwel tegelijkertijd uit het schap werd weggenomen, het slimme schap dit zou waarnemen en een signaal sturen naar een bewakingscamera die dan opnamen maakte van de vermoedelijke diefstal. Ook kon direct het winkelperso-

[19] NB. RFID is een peer-to-peer-verbinding, geen telecommunicatieverbinding.

neel worden ingeseind. Na protesten van de zijde van consumentenorganisaties werd deze test echter weer stopgezet. De test laat echter wel de kracht van RFID zien en de creativiteit van sommige toepassingen ervan.

3.7 Medische omgevingen/farmaceutische industrie

In medische omgevingen kan RFID een krachtig hulpmiddel zijn om (dodelijke) ongelukken te voorkomen. Men moet dan denken aan het identificeren van patiënten door middel van RFID-polsbandjes. De polsbandjes moeten voorkomen dat de patiënt in de operatiekamer de verkeerde behandeling ondergaat omdat zijn identiteit en zijn dossier verwisseld worden met die van iemand anders. En door operatiegereedschap van een RFID-chip te voorzien, valt het gereedschap sneller te lokaliseren en kan worden gegarandeerd dat er na een operatie geen gereedschap per ongeluk in de patiënt achterblijft.
Ook medicijnen worden van een RFID-chip voorzien. Daarmee kunnen verschillende doelen gediend worden. Het helpt enerzijds het medisch personeel om de juiste medicijnen aan de juiste patiënt toe te dienen en dus een het aantal (dodelijke) gevallen van verkeerd toegediend medicijngebruik te verminderen. Anderzijds kan RFID op medicijnen in combinatie met een slim medicijnkastje ook bijdragen aan een grotere zelfstandigheid van zieke en bejaarde mensen omdat het mogelijk is om het monitoren van medicijngebruik te automatiseren. Indien een dosis wordt gemist, kan automatisch de dokter of een familielid worden gewaarschuwd.
Voorts is het mogelijk om RFID-chips in combinatie met sensortechnologie en telecommunicatiemiddelen (telefoon, internet) in te zetten voor 24-uurs gezondheidsbewaking. Te denken valt bijvoorbeeld aan 24-uurs hartbewaking als service waarop een hartpatiënt zich kan abonneren, of het op afstand monitoren van patiënten terwijl zij in hun thuisomgeving herstellen van een operatie. Daarmee kan de dure en schaarse ziekenhuiscapaciteit beter benut worden.
Ten slotte – en niet onbelangrijk omdat het op korte termijn een van de belangrijkste toepassingen van RFID zal worden – kan RFID helpen om het gigantische probleem van nagemaakte geneesmiddelen terug te dringen. Door RFID kan steeds de herkomst en de echtheid van een medicijn worden bepaald. Dit moet helpen om (dodelijke) ongelukken als gevolg van het gebruik van verboden of namaakmedicijnen terug te dringen.

3.8 E-purse en betaalsystemen

Een belangrijke toepassing van contactloze smart cards is contactloos betalen met een RFID-chip gebaseerd op het NFC-protocol. Aan contactloos betalen zijn een paar grote voordelen verbonden. Zo is de levensduur van een pasje met RFID aanzienlijk langer dan die van een pasje met een magneetstrip. We kennen het allemaal: de magneetstrip van het bank- of giropasje dat het bij het pinnen laat afweten of een chipknip die kapot is. Dat zal door RFID tot het verleden behoren omdat RFID in het plastic van de kaart kan worden geïntegreerd waardoor het niet of nauwelijks onderhevig is aan slijtage.
Verder heeft het gebruik van RFID in creditcards nog het voordeel dat de consument zijn pasje niet meer hoeft af te geven bij een betaling. Hij kan zelf met zijn pasje langs een (mobiel) leesapparaat wapperen en de transactie autoriseren.
Een contactloze smart card kan naast het fungeren als modern bankpasje of moderne creditcard, ook gebruikt worden als zogeheten e-purse of elektronische portemonnee. Net als bij de chipknip worden op de e-purse 'credits' geladen, die corresponderen met een bepaalde hoeveelheid geld en die bij een betaling in het geheugen van de chip worden afgeboekt. De e-purse functie kan gebruikt worden om te betalen in bedrijfskantines, benzinestations (te denken valt aan de Shell's Easypay of Exxon's Speedpass), maar kan ook worden gebruikt om losse openbaar vervoertickets op te laden of om spaarpunten op te slaan. Ten slotte kan de e-purse functie van RFID-chips gebruikt worden bij tolpoortjes en rekeningrijden.
Door een e-purse te combineren met NFC in een telefoon of PDA, wordt nog een ander belangrijk knelpunt in elektronisch betalen opgelost, en wel het punt van het vertrouwen in de autorisatie van de betaling. Thans is het zo dat bij creditcards, chip en PIN-transacties de autorisatie van de betaling plaatsvindt op of in het systeem van de winkelier (denk aan het intoetsen van de pincode en de OK-knop). Met NFC in een telefoon of PDA (of een ander apparaat met een user interface) kan de consument de transactie in zijn *eigen* apparaat autoriseren, hetgeen fraude met elektronische betalingen aanzienlijk moet terugdringen. Hiermee zal de consument meer vertrouwen krijgen in creditcards en elektronisch betalen.

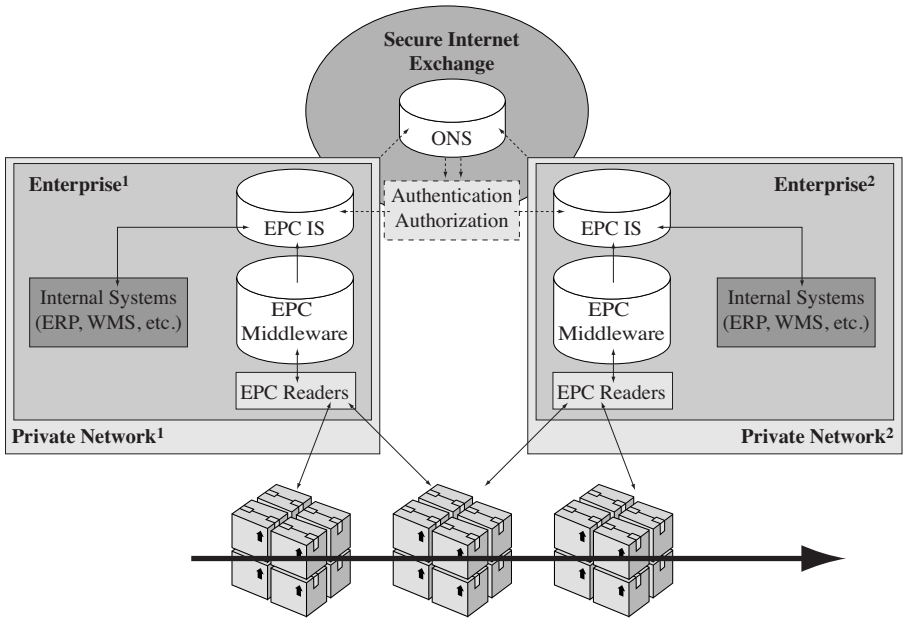
3.9 Supply chain management/EPC

De allerbelangrijkste toepassing van RFID in de toekomst is ongetwijfeld die in supply chain management als vervanger van de barcode. Op dit moment moet de barcode van iedere container, iedere pallet, iedere doos of ieder product met de hand worden gescand, of – als het al is geautomatiseerd – in ieder geval item voor

item, hetgeen veel capaciteit en tijd, en dus veel geld kost. RFID belooft een gigantische efficiencyverbetering teweeg te brengen in de logistieke ketens van organisaties. Doordat in enkele seconden iedere RFID-chip op een pallet gelezen kan worden door een netwerk van onderling verbonden leesapparaten, weet een organisatie precies welk goed zich op welk moment waar bevindt. Daar komt nog bij dat het voorraadbeheer ook aanzienlijk wordt verbeterd, zodat consumenten minder vaak in de winkel lege schappen zullen aantreffen. Niet voor niets hebben Walmart (de grootste supermarktketen ter wereld) en het Amerikaanse Ministerie van Defensie van hun belangrijkste leveranciers geëist dat zij hun producten voorzien van RFID-chips. Ook in Nederland worden – zij het nog op beperktere schaal – reeds tests uitgevoerd voor toepassing van RFID in de logistieke keten.

Elke 'smart tag' is in principe geschikt voor supply chain management. Maar om tussen sectoren en landen tot integrale supply chain management oplossingen te komen, was een wereldwijde standaard noodzakelijk. De Auto-ID Labs, een samenwerkingsverband van een aantal universiteiten, kwamen met de oplossing: de *Electronic Product Code* (EPC), die zich met name concentreert op de UHF-band vanwege de relatief hoge snelheden en het grotere bereik, waardoor UHF uitermate geschikt is voor logistieke toepassingen. De EPC wordt daarom ook wel de 'vervanger van de barcode' genoemd. Door zowel de chiptechniek als de serienummers van de RFID-chips te standaardiseren, ontstaat de zogeheten EPC-chip. Deze chip heeft een 96-bit nummer dat is opgedeeld in delen: een landcode, een leverancierscode, een productcode, een serienummer (van het product binnen een bepaald productcode), eventuele additionele informatie (bijvoorbeeld houdbaarheidsdatum) en een controlegetal. Als een product met een EPC-chip een leesapparaat passeert, registreert het apparaat dit nummer en zendt dit door naar een computer die in real time het nummer via de Object Name Service (ONS) in het EPCglobal netwerk opzoekt.[20] De ONS stuurt die computer vervolgens door naar de EPC-IS computer van de juiste leverancier waarin additionele informatie over het product is opgeslagen, zoals bijvoorbeeld: naam, herkomst, productinformatie, prijs enzovoort. Het aantal gescande producten wordt door de computer zelf bijgehouden. Op die manier weet de computer van het leesapparaat in de supermarkt dus dat hij zojuist een rolcontainer met 10 kratten cola light van merk X, en 18 dozen met blikjes bier van merk Y heeft zien langskomen. In het onderstaande plaatje wordt de procedure nog eens schematisch weergegeven.

[20] De ONS werkt op dezelfde manier als de DNS (Domain Name Server) voor het opzoeken van internet URL's.



Bron: EPCGlobal Inc.

De organisatie die wereldwijd de standaarden bepaalt en het netwerk beheert, is EPCglobal Inc. EPCglobal is een onderdeel van GS1 (een samenwerkingsverband tussen de voormalige EAN en UCC), de wereldorganisatie voor numbering in de supply chain, die ook de barcodenummers in beheer heeft. Bij GS1 zijn meer dan 1 miljoen bedrijven, voornamelijk producenten, aangesloten.[21] Het is dus belangrijk om te beseffen dat er niet zoiets bestaat als een wereldwijde database met alle productgegevens erin. Het is uiteindelijk aan de producent van het product (en dus de eigenaar van de informatie) om te bepalen wie wel en wie niet toegang krijgt tot de informatie in zijn computers.

Na een voorzichtige start met de eerste generatie EPC-chips, is sinds kort een betere en meer gestandaardiseerde EPC-chip op de markt: de EPC Class 1 Gen 2.[22] De Gen 2 heeft een iets groter bereik (6 meter in plaats van 4 meter), en heeft een ingebouwde mogelijkheid om de chip te deactiveren (ook wel de 'kill-switch' genoemd). De kill-switch, wat eigenlijk een door het leesapparaat uitgezonden signaal is om het serienummer uit het geheugen van de chip te wissen,

21 Zie voor meer informatie: www.gs1.nl en www.epcglobalinc.org

22 Meer informatie over de Gen2-chip: www.semiconductors.philips.com/acrobat_download/literature/9397/75015301.pdf

zorgt ervoor de chip geen signaal meer teruggeeft als hij daarna wordt uitgelezen. De kill-switch is ingebouwd in de EPC Gen 2-standaard om de consument een mogelijkheid te bieden de chip bij het verlaten van de winkel te deactiveren (als natuurlijk de chip niet gewoon van het product kan worden verwijderd). Het deactiveringsproces is redelijk snel, omdat de chips van alle boodschappen tegelijk kunnen worden gedeactiveerd. De Internationale Kamer van Koophandel (ICC) heeft begin 2005 een richtlijn 'Principles for fair use of RFID/EPC' vastgesteld, waarin expliciet is aangegeven dat de consument moet worden gewezen op de aanwezigheid van RFID-chips, en hoe ze kunnen worden verwijderd of worden gedeactiveerd.[23]

3.10 De toekomst: 'Ubiquitous computing' en 'Ambient Technology'

Hoewel het idee van RFID al zo'n vijftig jaar oud is, staat de techniek qua toepassingen en ontwikkeling nog aan het begin van zijn levensfase. De uitrol van EPC in de wereldwijde supply chain zal binnen een paar jaar een feit zijn, maar nieuwe technieken en toepassingsmogelijkheden zullen ook niet lang op zich laten wachten. Met name de combinatie van RFID- en sensortechnologie zal een ware revolutie in onze samenleving teweegbrengen. De wereld om ons heen zal 'slim' worden en zich automatisch kunnen aanpassen op onze voorkeuren. Te denken valt aan de auto die onze instellingen van de stoel-, stuur- en spiegelpositie onthoudt, zodat je alleen nog hoeft in te stappen (toegegeven: op basis van de RFID nu in de sleutel, zodat even je auto aan je buurman uitlenen er niet meer echt inzit). Verder is natuurlijk de slimme wasmachine hét voorbeeld van 'ambient technology'. De wasmachine kiest zelf het juiste wasprogramma op basis van de informatie in de RFID-labels in de kleding, en waarschuwt als er twee kledingstukken samen in de wasmachine zitten die beter apart kunnen worden gewassen ('de rode sok en het witte overhemd'). De slimme magnetron weet hoe die een kant-en-klaar-maaltijd moet bereiden, en de slimme koelkast houdt in de gaten of onze minimale voorraad melk en boter nog wel aanwezig is of dat de eieren wellicht bedorven zijn. Door de koelkast te verbinden met het internet, kan het boodschappenlijstje alvast naar het slimme winkelwagentje worden gestuurd waar je met je RFID-klantenkaart aanlogt, en waar de wensen van de koelkast (melk, kaas, cola) samen met die van de badkamer (tandpasta, deodorant) en het

[23] Te vinden op www.iccwbo.org/id600/index.html

toilet (wc-papier) op een beeldscherm getoond worden. En natuurlijk zullen we de winkel verlaten door gewoon met ons winkelwagentje naar buiten te lopen en tegelijkertijd via RFID af te rekenen.
De verwachting is dat nog vele andere producten die wij in ons dagelijks leven gebruiken slim worden en wireless aangesloten zullen zijn op het Internet of telecomnetwerken. Maar de ontwikkeling van de technologie gaat nog verder. In laboratoria wordt gewerkt aan '*smart dust'*, minuscule chipjes die zelf in staat zijn om onderling netwerken te vormen. Het creëren en gebruiken van dergelijke netwerken wordt ook wel 'ubiquitous computing' genoemd.

3.11 RFID: het einde van de privacywetgeving?

Bij RFID-technologie en ubiquitous computing staan bestaande privacyconcepten als 'data controller', 'data processor' en 'doelbinding' onder druk. Op een onlangs gehouden OESO-conferentie over de toekomst van RFID-technologie werd dat door meerdere sprekers uitdrukkelijk erkend. Onze huidige zogenoemd 'technologieneutrale' privacyprincipes die dateren van de hoogtijdagen van de mainframecomputer en het begin van het Internettijdperk naderen het einde van hun houdbaarheid. Termen als 'electronic footprints' zullen verouderde termen als 'persoonsgegevens' gaan vervangen en de nadruk zal op het voorkomen van nadeel en misbruik komen te liggen.
RFID-technologie luidt naar mijn mening daarmee het einde in van bestaande regelgeving zoals de Europese dataprotectie richtlijn (95/46/EG), de (nog recente) Europese richtlijn voor elektronische communicatie en privacy (2002/58/EG), en onze Wet bescherming persoonsgegevens. De Artikel 29 Werkgroep heeft in haar werkdocument WP 105 een krampachtige (en naar mijn mening: mislukte) poging gedaan om RFID-technologie onder de reikwijdte van de bestaande privacywetgeving te brengen.[24] Vooralsnog zullen de bestaande wettelijke concepten voldoende zijn om het gebruik van gegevens die via RFID verzameld zijn, te reguleren. Maar de wet schiet al tekort waar het gaat om het verzamelen van gegevens via RFID-technologie. Aanpassen van de wet heeft echter

[24] Dit is echter geen probleem van RFID-technologie alleen. Ook het Internet toont de inherente tekortkomingen van het Europese compliance-model voor privacybescherming aan. De naar mijn mening eveneens mislukte *Bodil Lindqvist*-zaak van het Europese Hof van Justitie inzake de doorgifte van gezondheidsgegevens via een website, is hier een overduidelijk voorbeeld van. EHvJ, 6 november 2003, C101/01. Zie daarover o.a. G-J. Zwenne, 'Bodil Lindqvist', *JAVI* 2004-2, p. 66-70; P. Blok, 'Inkomens, internet en informationele privacy, *NTER* 2004-1/2, p. 30-36; J.M.A. Berkvens, 'De Lindqvist-case of de onbevlekte ontvangenis van persoonsgegevens', *Privacy en Informatie* 2004-1, p. 17-20; H. Kranenborg, 'Pas op met wat je op je homepage zet!' *NJCM-bulletin* 2004-3.

geen zin. Naar mate RFID meer en meer gebruikt zal gaan worden door mensen in hun privé-domein, en niet alleen door bedrijven en organisaties, zal de wettelijke uitzondering van 'persoonlijk en huiselijk gebruik' (artikel 2, onder a, Wbp) ook steeds vaker toepassing vinden. De privacy-issues zullen echter gewoon blijven bestaan.

Om de privacy-issues van RFID-technologie en straks van ubiquitous computing te kunnen adresseren, zullen we in Europa dus af moeten van het huidige compliance-model voor privacybescherming en moeten gaan naar een model dat bestaat uit de volgende drie lagen:

1 Privacy by design-oplossingen in technologie en standaarden,
2 Privacy by design-oplossingen is besluitvorming en implementatie (business modellen, systeemintegratie), en
3 wettelijke regels om nadeel en schade te adresseren (het 'harm'-model).

De grote uitrol van RFID-technologie (EPC) wordt verwacht over een jaar of vijf. Om dan klaar te zijn, zullen we dus nu al aan de slag moeten om het gebruik ervan (niet de technologie zelf !!) en de daaraan verbonden privacyaspecten te kunnen behappen.

4 De Wbp en RFID

Peter Blok

4.1 Inleiding

De Wet Bescherming Persoonsgegevens (Wbp) regelt een zorgvuldige omgang met persoonsgegevens. De wet is van toepassing ongeacht de techniek waarmee de persoonsgegevens worden verwerkt. Het voordeel van deze techniekonafhankelijke formulering van de regels van de Wbp is dat die regels ook een normatief kader kunnen bieden voor relatief nieuwe technieken, zoals bepaalde RFID-toepassingen. Het nadeel van de techniekonafhankelijke formulering is dat in bepaalde gevallen niet direct duidelijk is hoe de abstracte regels van de Wbp moeten worden toegepast ten aanzien van een nieuwe techniek. In dit hoofdstuk zal worden gepoogd enige helderheid te scheppen over de toepassing van de Wbp op RFID-systemen. Achtereenvolgens zal worden uiteengezet wanneer de Wbp van toepassing is op RFID-systemen, welke rechten en plichten deze wet schept, en wie verantwoordelijk is voor de naleving daarvan. Het doel van dit hoofdstuk is niet om de Wbp uitputtend te behandelen,[25] maar een overzicht te geven van de belangrijkste elementen van de Wbp waarmee men rekening moet houden bij het gebruik van RFID-systemen.

4.2 Wanneer is de Wbp van toepassing?

De Wbp is van toepassing indien er *persoonsgegevens* worden verwerkt (artikel 2 Wbp). Het begrip persoonsgegeven definieert de wet als 'elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon' (artikel 1, sub a, Wbp). Het gebruik van RFID-toepassingen valt derhalve onder de reikwijdte van de Wbp indien er met die techniek gegevens worden verwerkt die op de een of andere manier kunnen worden herleid tot een individuele persoon. RFID-systemen kunnen deze persoonsgegevens op twee manieren verwerken: (a) door de persoonsgegevens op de RFID-tag te plaatsen en (b) door de gegevens op de RFID-tag te koppelen aan elders opgeslagen persoonsgegevens.

---

[25] Voor een uitputtende behandeling van de Wbp wordt verwezen naar A. Holleman e.a. (red.), *Handboek Privacy*, (losbl.) Deventer: Kluwer; J.M.A. Berkvens & R.J.M. van der Horst (red.), *Wet bescherming persoonsgegevens. Leidraad voor de praktijk*, (losbl.) Deventer: Kluwer.

Van een gegevensverwerking waarop de Wbp van toepassing is, is ten eerste sprake indien op de RFID-tag gegevens worden opgeslagen die identificatie van een persoon direct of indirect mogelijk maken. Als bijvoorbeeld op een smartcard de NAW-gegevens van een persoon of andere *identifiers* zijn opgenomen, kunnen de op de kaart opgeslagen gegevens worden gekwalificeerd als persoonsgegevens en zal de opslag van die gegevens op de kaart, het uitlezen en verder verwerken daarvan zonder meer vallen onder het toepassingsbereik van de Wbp.
Ten tweede is de Wbp van toepassing op een RFID-systeem indien de gegevens op de RFID-tag kunnen worden gekoppeld aan elders opgeslagen persoonsgegevens. Zo kan in een database vastgelegd zijn dat een RFID-tag (bijvoorbeeld een toegangspas) die herkenbaar is aan een uniek nummer, is toegekend aan een bepaald persoon. In dat geval kan iedereen die toegang heeft tot die database de gegevens over het gebruik van de toegangspas die met behulp van de RFID-lezer worden geregistreerd, koppelen aan die persoon. Het verzamelen en verder verwerken van de gegevens is dan onderworpen aan de Wbp.
Om de koppeling tussen een RFID-tag en persoonsgegevens te leggen hoeft die tag niet te zijn uitgereikt door de gebruiker van een RFID-lezer. Een winkelier kan het verband bijvoorbeeld ook leggen door bij de kassa met een RFID-toepassing de producten in een boodschappenwagen te registreren en die te koppelen aan de via een klantenkaart geregistreerde persoonsgegevens. Op dergelijke gegevensverwerkingen is de Wbp van toepassing.

In veel gevallen zullen noch op de RFID-tag, noch in een database waarmee het RFID-systeem verbonden is, persoonsgegevens voorkomen. Zo werkt het systeem van EPC Global Network op basis van *smartlabels* waarop niet meer dan een uniek nummer, de zogenoemde *Electronic Product Code*, staat. Deze nummers maken het mogelijk een gelabeld product bijvoorbeeld te koppelen aan online beschikbare productinformatie. Deze RFID-toepassing valt in beginsel niet onder het bereik van de Wbp. Op de tag staan immers geen persoonsgegevens en de online beschikbare productinformatie heeft betrekking op producten in plaats van personen, en is derhalve geen persoonsgegeven.
Anders dan soms wordt aangenomen, maakt het enkele feit dat iemand een koppeling kan leggen tussen een product en een persoon niet dat gegevens betreffende dat product zijn aan te merken als persoonsgegevens. De Memorie van Toelichting op de Wbp stelt expliciet: ‘niet elk toevallig of technisch verband tussen een gegeven en een persoon is voldoende om dat gegeven een persoonsgegeven te doen zijn’.[26]

[26] *Kamerstukken II* 1997-1998, 25 892, nr. 3, p. 47.

Daarbij noemt de minister het voorbeeld van gegevens betreffende onroerende zaken. Het feit dat deze zaken via het kadaster of een ander openbaar register tot een individuele persoon kunnen worden herleid, maakt niet dat die zaaksgegevens persoonsgegevens zijn, aldus de minister. Hetzelfde geldt uiteraard voor gegevens betreffende roerende zaken, zoals boodschappen of kleding. Het feit dat deze zaken in verband kunnen worden gebracht met een bepaald persoon, bijvoorbeeld omdat iemand kan zien dat een persoon de producten bij zich draagt, maakt niet dat informatie over de eigenschappen van die producten persoonsgegevens zijn, ook niet als die productinformatie met behulp van een RFID-toepassing is verzameld.
De Wbp is wel van toepassing indien gegevens die strikt genomen betrekking hebben op een product, worden gebruikt om gegevens over een persoon te verzamelen. Dat is bijvoorbeeld het geval indien iemand weet dat een bepaald persoon een met een RFID-tag uitgerust product bij zich draagt, en vervolgens de gangen van die persoon nagaat door vast te leggen wanneer het product ergens is gesignaleerd. In dat geval verwerkt die persoon de productgegevens als ware het persoonsgegevens en zal hij dus gebonden zijn aan de Wbp.

4.3 Wie is waarvoor de verantwoordelijke?

De belangrijkste verplichtingen van de Wbp rusten op de verantwoordelijke. De verantwoordelijke wordt in artikel 1, sub d, Wbp gedefinieerd als ‘de natuurlijke, persoon, rechtspersoon of ieder ander die of het bestuursorgaan dat, alleen of tezamen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt’. De verantwoordelijke is dus degene die de zeggenschap heeft over de gegevensverwerking.
Indien er persoonsgegevens op de RFID-tag staan, zal degene die de persoonsgegevens op de tag heeft gezet (of heeft laten zetten) in het algemeen de verantwoordelijke zijn. Die persoon kiest immers voor de RFID-tag als een middel om de persoonsgegevens op te slaan en bepaalt welke gegevens er op de tag komen. Verder kan diegene ervoor kiezen de toegang tot de gegevens op de tag te beperken met encryptie of de gegevens toegankelijk te maken voor iedereen die een RFID-lezer heeft.
Voor het overige zullen de mogelijkheden van de verantwoordelijke om te bepalen wat er met de gegevens op de RFID-tag gebeurt veelal beperkt zijn, omdat de tag in het algemeen door iemand anders wordt beheerd. Het bijzondere is dat de feitelijke beheerder van de gegevens veelal de betrokkene, dat wil zeggen de persoon op wie de gegevens betrekking hebben, zal zijn (in plaats van een bewerker die de gegevens verwerkt namens de verantwoordelijke). In het algemeen zal een

RFID-tag waarop persoonsgegevens staan namelijk met de betrokkene worden meegegeven, bijvoorbeeld als een klantenkaart, toegangspas of elektronische strippenkaart. De betrokkene bepaalt vervolgens grotendeels zelf wat er met de gegevens gebeurt. Zo kan de betrokkene de kaart aan derden ter beschikking stellen, de beveiliging kraken en de gegevens mee naar het buitenland nemen (bijvoorbeeld naar landen zonder adequaat niveau van privacybescherming). Degene die de RFID-tag ter beschikking heeft gesteld zal in het algemeen weinig invloed kunnen uitoefenen op die handelingen van de betrokkene. Dat impliceert dat degene die de persoonsgegevens op de tag heeft gezet in beginsel niet zal kunnen worden aangemerkt als de verantwoordelijke ten aanzien van hetgeen de betrokkene met de tag doet.
Indien de persoonsgegevens zijn opgeslagen in een database die is gekoppeld aan een RFID-systeem is de verantwoordelijkheidsverdeling niet anders dan ten aanzien van andere databases. De beheerder van de database is in beginsel de verantwoordelijke ten aanzien van alle verwerkingen van de in de database opgenomen gegevens, met in begrip van de verzameling van de gegevens met behulp van het RFID-systeem. Die verantwoordelijkheid ontstaat zodra er gegevens met de RFID-lezer zijn verzameld.

4.4 Wanneer is het gebruik van een RFID-toepassing toegestaan?

Een belangrijk deel van de huidige privacyrechtelijke discussie over RFID-systemen gaat over de vraag of een opt-in (uitdrukkelijke voorafgaande toestemming van betrokkene) of een opt-out (stilzwijgende toestemming totdat betrokkene die uitdrukkelijk intrekt) nodig is. De voorvraag of de Wbp toestemming van de betrokkene, in welke vorm dan ook, vereist, wordt dan overgeslagen. Die vraag is met name van belang omdat toestemming niet het uitgangspunt, maar de uitzondering van het stelsel van de Wbp is. De Wbp biedt vele mogelijkheden om persoonsgegevens te verwerken zonder de toestemming van betrokkene. Bovendien eist de Wbp dat toestemming vrijwillig is gegeven en te allen tijde weer kan worden ingetrokken (zie artikel 1, sub i en artikel 5, tweede lid, Wbp). Dit laatste impliceert dat het vragen van toestemming moet worden gereserveerd voor die situaties waarin het al dan niet verwerken van persoonsgegevens daadwerkelijk kan afhangen van de keuze van de betrokkene. Bij veel RFID-toepassingen zal dat niet het geval zijn.
De toestemming van de betrokkene is niet nodig indien de verwerking van persoonsgegevens noodzakelijk is voor een van de in artikel 8, sub b-f, Wbp

genoemde doeleinden, waaronder de uitvoering van een overeenkomst (sub b), de vervulling van een publieke taak van een bestuursorgaan (sub e) en het gerechtvaardigd belang van de verantwoordelijke of een derde (sub f). Onder die laatstgenoemde grondslag vallen alle reguliere bedrijfsactiviteiten, met inbegrip van marktonderzoek, fraudebestrijding en bepaalde vormen van direct marketing (dat laatste onverminderd het recht van verzet op grond van artikel 41 Wbp en de spamregels van artikel 11.7 Telecommunicatiewet).[27] Aangezien de meeste RFID-toepassingen zullen worden gebruikt in het kader van de uitvoering van een overeenkomst, de vervulling van een publieke taak of reguliere bedrijfsactiviteiten vallen de meeste toepassingen onder een van de grondslagen van artikel 8, sub b-f, Wbp en is de voorafgaande toestemming van de betrokkene derhalve in beginsel niet vereist.

Artikel 8 Wbp eist echter ook dat de gegevensverwerking *noodzakelijk* is voor die doeleinden. Dat betekent dat de gegevensverwerking moet worden getoetst aan de beginselen van proportionaliteit en subsidiariteit. De subsidiariteittoets brengt onder meer mee dat moet worden aangetoond dat het noodzakelijk is om *persoons*gegevens te verwerken voor een bepaald doel en dat niet kan worden volstaan met anonieme gegevens. Indien bijvoorbeeld een detaillist door middel van een RFID-toepassing inzicht wil krijgen in het koopgedrag van zijn klanten teneinde zijn winkelinrichting of marketingbeleid daarop af te stemmen, is het veelal niet nodig om de klant te kunnen identificeren.[28] Anonieme profielen volstaan voor dat doel. Hetzelfde geldt indien een toegangspas met een RFID-tag uitsluitend als sleutel wordt gebruikt. Het kan onder omstandigheden uiteraard noodzakelijk zijn om te registreren wie zich wanneer toegang heeft verschaft tot een bepaalde ruimte, maar als dat niet het geval is, verbiedt de Wbp het gebruik van toegangspassen die herleidbaar zijn tot een bepaalde persoon. Ook los van artikel 8 Wbp is het voor de verantwoordelijke overigens zinvol om na te gaan of een bepaalde RFID-toepassing ook mogelijk is op anonieme basis, aangezien de Wbp niet van toepassing is op anonieme gegevensverwerkingen.
Verder verplicht artikel 11 Wbp de verantwoordelijke om uitsluitend accurate en relevante persoonsgegevens te verzamelen. Op grond hiervan dient de verantwoordelijke zich af te vragen of alle gegevens die met behulp van de RFID-toepassing kunnen worden verzameld, relevant zijn voor het doeleinde waarvoor de RFID-toepassing wordt gebruikt. Als een RFID-tag bijvoorbeeld slechts wordt

27 *Kamerstukken II* 1997-1998, 25 892, nr. 3, p. 86-87.

28 Vergelijk de discussie over de AH Bonuskaart: Registratiekamer 18 februari 1998, uitspraak z1997-0034.

gebruikt als een identificatiemiddel van de betrokkene, zal het niet altijd nodig zijn om vast te leggen waar en wanneer de tag is geregistreerd.
Voor de volledigheid wijs ik erop dat er bijzondere regels gelden voor de verwerking van privacygevoelige gegevens, zoals medische gegevens en strafrechtelijke gegevens (artikel 16 e.v. Wbp). Deze regels voor de omgang met deze gegevens zijn strikter, maar ook ten aanzien van bijzondere gegevens geldt dat de toestemming van de betrokkene niet altijd noodzakelijk is.

4.5 Welke beveiligingsmaatregelen moet de verantwoordelijke treffen?

Op grond van artikel 13 Wbp dient de verantwoordelijke passende technische en organisatorische maatregelen te nemen om persoonsgegevens te beveiligen tegen onrechtmatige verwerkingen. Dit heeft onder meer tot gevolg dat de verantwoordelijke dient te waarborgen dat de door hem verwerkte persoonsgegevens in beginsel uitsluitend door bevoegde personen worden verwerkt voor de doeleinden waarvoor de gegevens zijn verzameld.
Ten aanzien van RFID-toepassingen betekent dit dat de verantwoordelijke de nodige (technische) beveiligingsmaatregelen moet nemen. Indien de verantwoordelijke persoonsgegevens op een RFID-tag heeft gezet, zal die tag in het algemeen met encryptie moeten worden uitgerust teneinde te voorkomen dat iedereen met een RFID-lezer toegang kan krijgen tot de gegevens.
Vanuit privacyoogpunt heeft het plaatsen van de persoonsgegevens op een tag die de betrokkene als een elektronisch dossier met zich mee draagt, overigens ook voordelen in vergelijking met het opslaan van gegevens in een centrale database. De betrokkene heeft in dat geval (zeker indien de afstand waarop de tag is uit te lezen beperkt is) inzicht ín en tot op zeker hoogte controle óver de toegang tot zijn dossier. Voor kwaadwillenden is het bovendien lastiger om de gegevens die verspreid zijn over duizenden tags te verzamelen, dan een centrale database te raadplegen.
Indien een RFID-systeem is gekoppeld aan een database met persoonsgegevens zal ook die database moeten worden beveiligd tegen onbevoegde kennisneming. De beveiligingseisen voor een aan een RFID-toepassing gekoppelde database verschillen echter niet van andere databases met persoonsgegevens.

4.6 Waarover moet de betrokkene worden geïnformeerd?

Vanuit het oogpunt van privacybescherming is een van de belangrijkste kenmerken van een RFID-systeem dat bepaalde RFID-toepassingen het mogelijk maken persoonsgegevens te verzamelen zonder dat de betrokkene daarvan op de hoogte is. De Wbp biedt daaraan in zoverre tegenwicht dat de Wbp in beginsel eist dat de betrokkene wordt geïnformeerd over de verwerking van zijn gegevens, ook indien de gegevens worden verzameld met een RFID-systeem.[29]
De in de Wbp opgenomen informatieplichten verschillen naargelang de persoonsgegevens worden verzameld 'bij de betrokkene' (artikel 33 Wbp) of op andere wijze (artikel 34 Wbp). Het onderscheid is van belang omdat er minder uitzonderingen op de informatieplicht bestaan indien de gegevens bij de betrokkene worden verzameld. Bij gegevensvergaring bij de betrokkene kan de verantwoordelijke zich er bijvoorbeeld niet op beroepen dat het informeren van de betrokkene onmogelijk is of een onevenredige inspanning kost. Bij andere wijzen van gegevensverwerking is die uitzondering wel van toepassing (artikel 34, vierde lid, Wbp).
Hoewel de betrokkene er in het algemeen 'bij' zal zijn indien er met behulp van een RFID-lezer gegevens over hem worden vergaard, is artikel 33 Wbp niet van toepassing op de meeste RFID-toepassingen. Blijkens de Memorie van Toelichting is dat artikel namelijk geschreven voor het geval dat de betrokkene zelf actief gegevens verstrekt.[30] Indien de betrokkene passief blijft en er buiten hem om persoonsgegevens worden verzameld, is er geen sprake van een gegevensverwerking 'bij de betrokkene'. De Memorie van Toelichting noemt onder meer het voorbeeld van een verantwoordelijke die persoonsgegevens verzamelt door eigen observatie of door registratie van het gebruik dat de betrokkene maakt van een netwerk dat onder het beheer van de verantwoordelijke valt. Aangezien bij de meeste RFID-lezers geen actieve handeling van de betrokkene nodig is, zullen de meeste RFID-toepassingen vallen onder artikel 34 Wbp. De uitzondering is wellicht het geval dat de betrokkene de RFID-tag actief langs een lezer moet halen om een gegevensuitwisseling mogelijk te maken.

De verantwoordelijke moet de betrokkene in beginsel informeren vóór of bij het verzamelen van de gegevens. Dat zou betekenen dat die informatie moet worden verstrekt op het moment dat de RFID-lezer een tag registreert, hetgeen nogal

---

[29] Het is onder omstandigheden ook toegestaan om persoonsgegevens te vergaren zonder de betrokkene te informeren. Voor dit heimelijke vergaren van persoonsgegevens is echter voorafgaande goedkeuring van het CBP vereist (artikel 31, eerste lid, sub b, Wbp).

[30] *Kamerstukken II* 1997-1998, 25 892, nr. 3, p. 149-150.

onpraktisch kan zijn en onder omstandigheden zelf een onevenredige inspanning kan meebrengen in de zin van artikel 34, vierde lid, Wbp. Bij de meeste RFID-toepassingen die onder de Wbp vallen, zal de verantwoordelijke echter al persoonsgegevens hebben verwerkt vóórdat er met een RFID-lezer gegevens worden verzameld. In dat geval ligt het voor de hand om de betrokkene op een eerder moment te informeren. Indien de verantwoordelijke bijvoorbeeld persoonsgegevens op een smart card van een klant zet, heeft de verantwoordelijke op dat moment logischerwijs al de beschikking over die gegevens. De verantwoordelijke kan de betrokkene dan informeren over de RFID-toepassing op het moment dat die gegevens worden verzameld of eventueel bij de uitreiking van de smart card. Ook indien de persoonsgegevens zijn opgenomen in een database die is aangesloten op een RFID-systeem zal de verantwoordelijke veelal al persoonsgegevens van de betrokkene verwerken op het moment dat de RFID-lezer gegevens vastlegt. Ook in dat geval kan de verantwoordelijke op een eerder moment aan de informatieplicht voldoen door bij het verzamelen van de database opgenomen gegevens de betrokkene te melden dat die gegevens kunnen worden verrijkt met gegevens die de verantwoordelijke met behulp van een RFID-toepassing verzamelt.

De verantwoordelijke moet de betrokkene informeren over diens identiteit en de doeleinden waarvoor de gegevens worden verwerkt. Daarnaast moet de betrokkene alle informatie krijgen die, mede gelet op de omstandigheden waaronder de gegevens zijn verkregen, 'nodig is om tegenover de betrokkene een behoorlijke en zorgvuldige verwerking te waarborgen' (artikel 33, derde lid, en 34, derde lid, Wbp). Gezien de relatieve onbekendheid van RFID-toepassingen voor de gemiddelde betrokkene, moet worden aangenomen dat op grond hiervan de verantwoordelijke de betrokkene in beginsel zal moeten informeren over het gebruik van een RFID-systeem en kort uitleggen welke consequenties dat heeft voor de betrokkene. Zo lijkt het gepast dat indien er persoonsgegevens op een smart card van de betrokkene worden gezet, de betrokkene krijgt uitgelegd wie wanneer toegang kan krijgen tot die gegevens. Indien de verantwoordelijke de met een RFID-systeem verzamelde productinformatie kan koppelen aan een persoon, dient te worden uitgelegd welke categorieën van producten zijn uitgerust met een tag en waar die kunnen worden uitgelezen. Een praktische manier om daar invulling aan te geven is het plaatsen van een pictogram op de gelabelde producten en op de plaats waar een RFID-lezer zich bevindt.

4.7 Welke rechten heeft de betrokkene?

De Wbp geeft de betrokkene recht op inzage en correctie van diens persoonsgegevens. Het recht op inzage is geregeld in artikel 35 Wbp. Dit artikel verplicht de verantwoordelijke de betrokkene mee te delen of er persoonsgegevens worden verwerkt en indien er persoonsgegevens worden verwerkt, daarvan een 'overzicht' in begrijpelijke vorm te geven. Anders dan de artikel 29-werkgroep in haar rapport over RFID heeft gesuggereerd, geeft artikel 35 de betrokkene geen recht op 'inzage' van de tag (tag content access).[31] Nog afgezien van het feit dat de betrokkene door directe toegang tot de tag veelal geen informatie in begrijpelijke vorm zal ontvangen, verplicht het artikel de verantwoordelijke niet tot het geven van directe toegang tot de bron van de gegevens. Het volstaat dat de verantwoordelijke een overzicht kan verschaffen van de categorieën van persoonsgegevens die op een tag (of in een database) zijn opgenomen.[32] Dit laat natuurlijk onverlet dat het ontwerpen van een RFID-display waarmee de op een tag opgeslagen gegevens direct voor de betrokkene inzichtelijk kunnen worden gemaakt, een handige manier is om het verplichte overzicht te geven. De Wbp dwingt echter niet tot die wijze van implementatie.
Hetzelfde geldt voor het recht op correctie. Artikel 36 Wbp verplicht de verantwoordelijke op verzoek van de betrokkene gegevens te verbeteren, aan te vullen, te verwijderen of af te schermen voorzover de gegevens feitelijk onjuist zijn, voor het doel of de doeleinden van de verwerking onvolledig of niet ter zake dienend zijn dan wel anderszins in strijd met een wettelijk voorschrift worden verwerkt. De verantwoordelijke dient zorg te dragen voor de uitvoering van een dergelijk verzoek. De verantwoordelijke hoeft de betrokkene echter niet de technische middelen te verschaffen om bijvoorbeeld de op een RFID-tag gezette persoonsgegevens zelf te kunnen aanpassen.

Ten slotte bieden de artikelen 40 en 41 Wbp de betrokkene een recht op verzet, maar met uitzondering van gegevensverwerking in het kader van direct marketing (artikel 41, Wbp), is dat verzetsrecht niet absoluut. Het verzetsrecht van artikel 40 Wbp verplicht de verantwoordelijke slechts om de verwerking van iemands persoonsgegevens te heroverwegen indien de betrokkene 'bijzondere persoonlijke omstandigheden' kan aandragen die meebrengen dat een op zich gerechtvaardigde gegevensverwerking ten aanzien van die betrokkene niet is toe-

---

31 Article 29 Data Protection Working Party 19 januari 2005, Working document on data protection issues related to RFID Technology, WP105.

32 Vergelijk Rb. Breda 1 april 2005, LJN AT3948 (artikel 35 schept geen recht op kopieën van vastgelegde gegevens).

gestaan. Dit recht is dus per definitie slechts in uitzonderingsgevallen van toepassing.
Een algemeen recht van verzet geldt wel indien de gegevensverwerking is gebaseerd op de toestemming van de betrokkene (opt-in of opt-out). In dat geval heeft de betrokkene het recht om zijn al dan niet stilzwijgende toestemming in te trekken. Ook hier geldt dat de verantwoordelijke niet verplicht is om de betrokkene de technische middelen te verschaffen om de gegevensverwerking eigenhandig te staken. Het volstaat dat de verantwoordelijke de gegevensverwerking op verzoek van de betrokkene beëindigt. Indien er persoonsgegevens op de RFID-tag staan, kan de verantwoordelijke eenvoudig aan dat verzoek voldoen door de tag in te nemen en de daarop staande gegevens te vernietigen. Indien er met een RFID-systeem verzamelde informatie wordt gekoppeld aan persoonsgegevens, kan de verantwoordelijke de gegevensverwerking beëindigen door die koppeling onmogelijk te maken. Nog afgezien van het feit dat voor de meeste RFID-toepassingen geen toestemming is vereist (en er derhalve geen absoluut verzetsrecht geldt), zal de introductie van een zogenaamde *kill switch*, waarmee de betrokkene zelf een RFID-tag onklaar kan maken, in het algemeen dus niet zijn vereist op grond van de Wbp.

4.8 Wat moet er worden gemeld bij het CBP?

In beginsel moet elke verwerking van persoonsgegevens met behulp van een RFID-toepassing worden gemeld bij het CBP (artikel 27 Wbp). Er bestaat echter een reeks van vrijstellingen op de meldingsplicht voor standaardgegevensverwerkingen, zoals klantenbestanden en personeelsadministraties die aan bepaalde voorwaarden voldoen (artikel 29 Wbp). Deze staan opgesomd in het zogeheten Vrijstellingsbesluit Wbp (Vb). De vrijstellingen zijn in het algemeen techniekonafhankelijk geformuleerd, zodat ook gegevensverwerkingen met behulp van RFID-technologie in aanmerking kunnen komen voor een vrijstelling van de meldingsplicht.
Zo bestaat er een vrijstelling voor gegevensverwerkingen in het kader van toegangscontrole (artikel 35 Vb). Op grond van deze vrijstelling mag een verantwoordelijke gegevens over onder meer ‘het feitelijk gebruik van verleende bevoegdheden’ registreren met het oog op controle van de toegang tot gebouwen en informatiesystemen. Het Vrijstellingsbesluit stelt geen voorwaarden aan de wijze waarop de gegevens over het gebruik van verleende bevoegdheden wordt geregistreerd. De vrijstelling van de meldingsplicht vervalt dus niet indien de

verantwoordelijke in dat kader gebruikmaakt van toegangspassen voorzien van een RFID-tag en RFID-lezers.
Ook de vrijstelling voor klantenbestanden kan van toepassing zijn indien er gebruikgemaakt wordt van RFID-technologie (artikel 13 Vb). Onder deze vrijstelling kan een verantwoordelijke onder meer gegevens verwerken met het oog op het doen van leveringen en het berekenen en vastleggen van inkomsten. Een winkel kan die gegevens bijvoorbeeld verzamelen met behulp van een RFID-lezer die registreert welke producten iemand in zijn winkelwagen heeft. Gekoppeld aan de via een klantenkaart of bankpas verzamelde persoonsgegevens van een klant mag de winkelier die gegevens gebruiken overeenkomstig de voorwaarden van artikel 13 Vb zonder zich te hoeven melden bij het CBP.
Ervan uitgaande dat de meeste RFID-toepassingen vallen onder een bestaande vrijstelling, lijkt een specifieke vrijstelling voor RFID-systemen vooralsnog niet nodig.

5 Zorg en RFID

Roel Croes

5.1 Inleiding

In de huidige situatie wordt RFID nog niet specifiek toegepast in de zorg. Hierop zijn twee uitzonderingen. Allereerst wordt RFID wel toegepast voor 'tracken en tracen' in de logistieke keten, waarbij bijvoorbeeld een ziekenhuis de rol van eindgebruiker vervult. Dit is echter geen specifieke zorgtoepassing. Verder zijn er toepassingen in experimentele of testomgevingen. Deze testomgevingen zijn over het algemeen dermate kleinschalig dat aanpassing van regelgeving of juridische systemen niet aan de orde is. Met betrekking tot lacunes in regelgeving kunnen deze testomgevingen echter wel een goede 'eye-opener' zijn.

In dit hoofdstuk wordt een beschrijving gegeven van een aantal reeds gerealiseerde en nog te realiseren RFID-toepassingen in de zorgsector. Hierbij wordt een onderscheid gemaakt tussen persoonsgebonden toepassingen van RFID en objectgebonden toepassingen van RFID. Bij deze beschrijvingen wordt telkens aangegeven welke juridische vragen er bij de verschillende toepassingen aan de orde zijn en hoe deze zouden kunnen worden beantwoord. De toepassingsmogelijkheden van RFID-technologie in een medische omgeving zijn behoorlijk divers. Aan de hand van uiteenlopende voorbeelden, geef ik een niet-limitatieve beschrijving van huidige en mogelijk toekomstige toepassingen.

Zorgsector start proef met RFID
Op verzoek van het Ministerie van VWS en met steun van het Ministerie van EZ als coördinator van de Rijksbrede ICT-agenda start Capgemini een onderzoek naar de toepassingsmogelijkheden van RFID in de gezondheidszorg. Capgemini doet dit onderzoek samen met het Academisch Medisch Centrum (AMC), Geodan, Intel en Oracle. Het project duurt circa een jaar en bestaat uit inventarisatie- en standaardisatiewerkzaamheden en een drietal pilots. Doel van het onderzoek is de meerwaarde van RFID-toepassingen in de zorg aan te tonen.

De eerste twee delen van het project bestaan uit inventarisatie en standaardisatiewerkzaamheden. Doel hiervan is in beeld te brengen aan welke voorwaarden moet worden voldaan om een breder gebruik van RFID-technologie in de zorg mogelijk te maken. De standaardisatiewerkzaamheden geven inzicht in de ontwikkelingen op het gebied van technische en inhoudelijke standaarden voor RFID. Op basis hiervan kunnen Neder-

landse zorginstellingen worden geadviseerd over het gebruik van deze standaarden bij de toepassing van RFID.

Het laatste deel van het project bestaat uit drie pilots die de toegevoegde waarde van RFID in de zorgpraktijk moeten aantonen. De eerste pilot richt zich op personenidentificatie en -lokalisatie rond de OK (operatiekamer). De pilot moet beter inzicht geven in het verloop van het zorgproces op en rond de OK zodat de logistiek optimaal kan worden georganiseerd. Tevens zoekt men naar een snellere methode om patiënt en zorgverlener te identificeren. In combinatie met het tracken en tracen van OK-materialen en bloedproducten (de andere twee pilots, zie hieronder), kan zo de registratie van het verbruik van materialen, het gebruik van bepaalde apparatuur en de toediening van bloedproducten een stuk makkelijker verlopen.
De tweede pilot richt zich op het tracken en tracen van OK-materialen als implantaten en disposables met een hoge kostprijs en omloopsnelheid.[33] Doel is het verbruik per patiënt van deze producten te traceren zodat het voorraadbeheer kan worden geoptimaliseerd. Daarnaast is op langere termijn een bijdrage mogelijk aan de realisatie van Activity Based Costing. Door de toepassing van RFID wordt bovendien beter voldaan aan de wettelijke eisen met betrekking tot de traceerbaarheid van implantaten.
De derde pilot omvat het tracken en tracen van bloedproducten met behulp van temperatuurgevoelige RFID-tags. Doel hiervan is enerzijds het voldoen aan nieuwe Europese normen op het gebied van de traceerbaarheid en kwaliteit van transfusiebloedzakken. Anderzijds wil men meer efficiëntie bereiken door besparingen die volgen uit een verhoogde kwaliteit en door vermindering van het aantal handmatige acties zoals het nabellen over de procesgang.[34]

5.2 Persoons- en objectgebonden RFID-toepassingen

Grofweg kan men bij toepassingen van RFID in de gezondheidszorg een onderscheid maken in twee categorieën.[35] Enerzijds zijn er de toepassingen waarbij de band met de betrokken persoon voorop staat, de persoonsgebonden RFID-toepassingen.[36] In dergelijke situaties is de RFID-toepassing rechtstreeks gekoppeld aan een persoon. Men kan onder meer denken aan identificatiemiddelen en implantaten. Anderzijds is er de groep toepassingen waarbij objecten de meest

33 Een vergelijkbare pilot is reeds uitgevoerd, zie het kader 'Pilot study Biomet'.

34 <http://www.nl.capgemini.com/actueel/nieuwspers/2005/september/proef_RFID.htm>. Overname met toestemming Capgemini. Het belang van het onderzoeksproject voor de Nederlandse gezondheidszorg is groot volgens stuurgroep voorzitter Robert Stegwee: *'Op dit moment staat een aantal knelpunten in de zorg hoog op de politieke agenda. Denk aan de vergrijzing, de vermindering van het aanbod van zorgverleners, een sterke stijging van de kosten van de zorg en de wachtlijstproblematiek. Technologische innovaties in de zorg als de toepassing van RFID, geven mogelijk een deel van het antwoord op deze maatschappelijke knelpunten.'*

35 Overigens lijkt me niets in de weg te staan dit onderscheid ook in andere omgevingen toe te passen.

centrale rol spelen. De meest directe band is, in dit soort gevallen, die tussen de RFID-tag en een voorwerp. Voorbeelden hiervan zijn de huidige 'fysiek tastbare' dossiers, medicijnen en medische hulpmiddelen.
Voor wat betreft de implantaten is een kanttekening op zijn plaats. De allocatie in bovenstaande onderverdeling is duidelijk situatieafhankelijk. Wordt de tag alleen gebruikt om een implantaat tijdens het logistieke proces, waarvan de operatiekamer het beoogde eindstation is, te volgen, dan kan men spreken van een objectgebonden toepassing.[37] Van persoonsgebonden toepassingen zou sprake kunnen zijn, ingeval de functionaliteit van de tag een aanvang neemt nadat deze geïmplanteerd is. Verderop zal ik hier nader op ingaan. Dit onderscheid zou van belang kunnen worden ten aanzien van de juridische kant van de materie. Met name vanuit het oogpunt van privacy is het feit dat een identificatiemiddel gekoppeld is aan een persoon of aan een voorwerp van wezenlijk belang.
Naast de onderverdeling in persoons- en objectgebondenheid, kan men de RFID-tags in het algemeen in twee soorten onderverdelen: de actieve en de passieve tags. Mijn verwachting is dat, indien massale inzet gewenst is, met name de toepassing van de passieve tag een grote vlucht zal nemen.[38] Dit baseer ik op de aanzienlijk lagere kostprijs per tag.[39] Ook zijn er technologische voordelen. De low cost passieve RFID-tag heeft de prettige eigenschap 'write once' en 'read many' te zijn. De kans op manipulatie van de tag wordt daardoor sterk gereduceerd. Het enige echte risico dat nog resteert is de mogelijkheid van het klonen (kopiëren) van de tag.[40]
De passieve RFID-tag leent zich ook bij uitstek voor traceerdoeleinden waarbij de (totale hoeveelheid) elektromagnetische interferentie (EMI) op diverse gronden beperkt dient te blijven. Zorginstellingen zijn hiervan een schoolvoorbeeld. Men kan denken aan vertrouwelijkheid van de informatie (informatiebeveiliging; het tegengaan van skimming) en gevoeligheid van elektronische apparatuur (persoonsveiligheid; het voorkomen van gezondheidsrisico's) op bijvoorbeeld Inten-

---

36 Bewust is hier gekozen voor de term: 'persoonsgebonden RFID-toepassingen'. Zuiver juridisch-technisch zou de term: 'subjectgebonden RFID-toepassingen' misschien beter op zijn plaats zijn. Vanuit het oogpunt de patiënt te zien als een mens en niet als een lijdend voorwerp, acht ik persoonsgebonden hier beter op zijn plaats. Overigens is in de zorg de meest optimale interactie met, of meer specifiek: de benaderwijze ten opzichte van, de patiënt al sinds mensenheugenis een punt van discussie.

37 Zie het kader 'Pilot study naar toepasbaarheid van RFID in het logistieke proces van Biomet'.

38 Ten aanzien van deze toename van toepassingen zal de gezondheidszorg zeker niet achterblijven. Mijn verwachting is dat juist het tegendeel zich zal voordoen.

39 De prijs van een standaard RFID-tag inlay is inmiddels al lager dan € 0,08. De prijs van een complete tag nadert de psychologische grens van € 0,10 met rasse schreden.

40 Zie voor meer over klonen en de juridische inbedding in het huidige strafrecht hoofdstuk 7 over criminaliteit en RFID.

sive en Medium Care afdelingen. De beperking van de totale omvang van elektromagnetische straling hangt nauw samen met een andere eigenschap van de passieve RFID-tag. Dat is het feit dat de activering van de tag altijd afhankelijk is van de aanwezigheid van een compatible reader. De omgeving bepaalt dus of er radiosignalen worden vrijgegeven. In dergelijke situaties heeft de zorgomgeving de meest optimale controle over de hoeveelheid aanwezige radiosignalen.

5.3 Persoonsgebonden RFID-toepassingen

De toepassingsmogelijkheden van persoonsgebonden RFID-technologie in de zorgsector zijn legio. Twee in het oog springende categorieën worden hieronder nader beschreven: de patiëntenkaarten en RFID-implantaten. De patiëntenkaart trekt als potentiële uitloper van het, qua privacy gevoelig liggende, elektronisch patiënten dossier (EPD) de meeste aandacht. Mijn verwachting is dat op termijn de impact van de implantaten op de samenleving die aandacht zal doen verbleken.

5.3.1 De patiëntenkaart

Op dit moment is het gangbaar dat ieder ziekenhuis een eigen systeem van patiëntenkaarten gebruikt. Als men ooit geconfronteerd is geweest met een specialisme overschrijdende aandoening, dan is men bekend met het feit dat iedere ziekenhuisafdeling een eigen patiëntenkaart verstrekt. Vaak gebruiken ziekenhuizen naast deze afdelings- of specialisme gebonden kaarten ook nog een algemene patiëntenkaart, bijvoorbeeld in de vorm van een ponsplaatje. Het toepassen van RFID kan er mede toe bijdragen dat het uitwisselen van informatie tussen zorginstelling en patiënt eenvoudiger, overzichtelijker en veiliger wordt.

Een pas met een RFID-tag kan voorzien in een unieke identificatie en authenticatie voor patiënten op een vergelijkbare wijze als bij het EPD. De wirwar van kaarten maakt dan plaats voor één pasje waarmee alle hulpverleners in de zorginstelling uit de voeten kunnen. Als men deze mogelijkheden integreert in het EPD, waar men gebruik gaat maken van een unieke zorgverlener identificatie (UZI)[41] en unieke zorgverzekeraar identificatie (UZIVO),[42] zal zelfs naadloze transmu-

[41] Dat wil zeggen een unieke identificatie (via een UZI-nummer) en authenticatie (via een UZI-pas) voor zorgverleners.

[42] Dat wil zeggen een unieke identificatie (via een nummer) en authenticatie (via een pas of een systeemcertificaat) voor zorgverzekeraars.

rale zorgverlening mogelijk kunnen zijn. De patiënt krijgt dan één pas voor de communicatie met alle zorgaanbieders. De huidige regelgeving (onder andere de Wbp en de Wet op de geneeskundige behandelingsovereenkomst) is uiteraard onverkort van toepassing. Of een koppeling wordt gemaakt via een unieke code of met behulp van de NAW-gegevens zal, juridisch gezien, uiteindelijk geen andere situatie opleveren.[43]

Gezien de aard van de op de kaart of in een achterliggende database vastgelegde gegevens (veelal bijzonder gegevens in de zin van paragraaf 2 van de Wbp) is met name een goede beveiliging noodzakelijk. Deze beveiliging kan bestaan uit vier elementen.[44]
Het eerste element is een gedegen versleuteling van de data. Met de huidige stand van de techniek zou dit geen bijzondere problemen moeten opleveren. Natuurlijk zal men altijd beducht moeten zijn voor personen met minder fatsoenlijke bedoelingen.[45]
Het tweede element is de beperking van de data op de kaart. Een unieke code kan volstaan.[46] Deze korte datastring is eenvoudiger, of zo men wil flexibeler te versleutelen. Een ander niet te onderschatten voordeel van het gebruik van slechts een codenummer is, dat de inhoudelijke data de betrokken zorginstelling niet verlaat. Dit verkleint de kans op misbruik. Omdat skimming alleen een unieke code oplevert, kan men niet op zijn gemak de, van de kaart gekopieerde, inhoudelijke data gaan ontsleutelen.[47] Tevens kan volstaan worden met RFID-systemen die in de lagere frequentiebanden opereren. Deze systemen zijn over het algemeen goedkoper dan RFID-systemen die werken op hogere frequentiebanden.[48]
Het derde element kan bestaan uit bescherming op het gebied van elektromagnetische interactie. Met betrekking tot het specifieke signaal is het wenselijk de maximaal overbrugbare afstand tussen tagreader en tag te beperkt te houden. Hoe korter de afstand is waarop een tag maximaal uitleesbaar is, hoe meer controle de patiënt (of in het algemeen: de gebruiker) heeft over de in de kaart opgeslagen gegevens. Een RFID-systeem dat werkt op een van de lagere frequentiebanden,

---

43 Meer over RFID en de Wbp in hoofdstuk 4.

44 De hier beschreven elementen zijn geenszins een limitatieve opsomming. Men kan bijvoorbeeld ook aan toepassingen van biometrie denken. De door mij beschreven elementen geven de kaart een vergelijkbare functionaliteit als de huidige combinaties van ponsplaatjes en papieren patiëntenkaarten.

45 Op dit moment lopen er meerdere onderzoeken waarbij dit onderwerp een centrale rol speelt. Zie onder meer: <http://www.cs.ru.nl/peRFIDe/> en <http://www.senternovem.nl/iopgeneriekecommunicatie/projecten/>

46 Met het oog op beveiliging zal deze code niet rechtstreeks afleidbaar van of herleidbaar tot een burgerservicenummer (BSN) (zie ook http://www.programmabsn.nl/), of sofi-nummer dienen te zijn.

47 Zie nader over 'skimming' het hoofdstuk over Criminaliteit en RFID van Bart Schermer.

48 Bart Schermer gaat in het tweede hoofdstuk uitgebreider in op RFID-technologieën.

de low frequentie (LF) of high frequentie (HF) frequenties, geniet dan ook de voorkeur. De huidige EPCglobal Network-standaarden[49] zijn gebaseerd op de wensen van de logistieke sector, waarbij juist de relatief krachtige signalen en de hogere datatransmissie snelheid van de hogere frequentiebanden (UHF) de voorkeur genieten.[50] Daarnaast is de gestandaardiseerde wijze van dataopslag in de tag ook specifiek gericht op goederen (met name de zogenheten fast moving consumer goods). De EPCglobal-standaarden zijn dan ook op meerdere gronden ongeschikt voor persoonsgebonden zorgtoepassingen.
Een technische oplossing voor het probleem van elektromagnetische interactie kan gevonden worden in het creëren van een kleine 'Kooi van Faraday'. Een dergelijk elektromagnetisch pantser voor RFID-kaarten wordt al commercieel geproduceerd. Een Japans bedrijf heeft een dunne folie ontwikkeld die gebruikt kan worden om RFID-kaarten te beschermen tegen datadiefstal.[51] De folie bevat een dunne metalen laag die als beschermend schild elektromagnetische velden van buiten weert, zodat de RFID-tag niet ongewenst kan worden uitgelezen.
Een vierde element wordt gevormd door de mogelijkheid de voor het menselijk oog leesbare data op de kaart te beperken. In het huidige systeem vermeldt een algemene patiëntenkaart naast de naam en voorletters tevens de geboortedatum, het geslacht, het volledige adres, het telefoonnummer, het relatie- of patiëntnummer, de zorgverzekeraar en de huisarts. De afdelings- of specialismegebonden patiëntenkaarten vermelden hiernaast tevens de behandelend arts, de betrokken (sub)afdeling en de gemaakte afspraken. Deze informatie kan bij het gebruik van een RFID-tag in de kaart zelf worden opgeslagen, of in de achterliggende database. Het invoeren van een elektronische patiëntenkaart in deze uitvoering zou dus een aanzienlijk toename van de privacy kunnen opleveren. In de gehele (juridische) discussie over privacy wordt aan dit positieve punt weinig aandacht besteed.

Aanvullende diensten
Een dergelijke patiëntenkaart kan verder worden aangekleed met een koppeling naar parkeren, het aanvragen van telefoon en televisie en andere extra diensten, zoals het bezoek aan het restaurant, de kapper, de pedicure en dergelijke. Voor grotere zorginstellingen kan dit administratieve voordelen opleveren. Ik verwacht

[49] De EPCglobal-standaarden betreffen naast de wijze waarop de informatie draadloos wordt uitgewisseld ook de informatie op het label en recentelijk de software voor retail RFID-labels.
[50] De officiële schrijfwijze is EPCglobal. Volgens Google kan men echter beter zoeken naar EPC Global. Dit levert veel meer relevante 'hits' op.
[51] Toppan Printing Co., Ltd., Tokyo Japan.

overigens niet dat een huisarts van deze extra functionaliteit wild zal worden. Een consequentie is dat een derde een gestolen kaart, die niet als vermist geregistreerd en geblokkeerd is, kan gebruiken. Dit zou verstrekkende juridische gevolgen kunnen hebben. Voor dergelijke diensten is een aanvullende vorm van identificatie wenselijk. Dit kan bijvoorbeeld via een pincode.
Een andere mogelijkheid is de toevoeging van een chipcardfunctionaliteit. Ook hier kan men gebruikmaken van RFID-technologie. Wanneer extra functionaliteiten aan de patiëntenkaart worden toegevoegd, is het wel zaak deze verschillende functies op de kaart (en in de achterliggende databases) te scheiden met het oog op de privacy van de patiënt. Gezien de reikwijdte van dit hoofdstuk, laat ik dit verder buiten beschouwing.
Een interessant project in dit verband is de Parkinsonpas. Dit is een patiëntenkaart annex verzekeringspas op het formaat van een creditcard. Hierop zijn de belangrijkste gegevens van de patiënt vastgelegd zoals bijvoorbeeld het, door de specialist vastgesteld, stadium van de ziekte van Parkinson, het ziekteverloop, verzekeringsgegevens en gegevens over het medicijngebruik. Er bestaat een mogelijkheid om specifieke patiëntgegevens te kunnen opnemen, waarbij de patiënt bepaalt wie inzage krijgt in de gegevens. De patiëntidentificatie geschiedt met behulp van biometrie in de vorm van vingerafdrukherkenning. De patiënt heeft hierdoor een uniek identificeerbare toegang tot zijn eigen dossier en persoonsverwisselingen kunnen worden voorkomen.[52]

Vergelijkbare RFID-tokens
In het verlengde van de RFID-patiëntenkaart ligt de mogelijkheid om patiënten andersoortige RFID-tokens te geven zoals bijvoorbeeld een polsbandje. Qua uitvoering kan dit een exacte kopie van de kaart worden. Het enige verschil is dat het polsbandje aan de patiënt vastzit, waardoor de identificatie van de betrokkene makkelijker wordt. Ten opzichte van de huidige polsbandjes zal er geen sprake zijn van een vermindering van de privacy. Indien, door gebruik van de RFID-tag, minder voor het menselijk oog leesbare informatie op de polsband staat, neemt de privacy zelfs toe. De mogelijkheden van de RFID-polsband zijn vergelijkbaar met een polsband die voorzien is van een barcode. Door bewust voor proximity RFID-tags en readers te kiezen en de tag uit te rusten met encryptie, is ook ten opzichte van de barcode het veiligheidsrisico bij het gebruik van RFID niet groter. Als toepassingsmogelijkheden kan men denken aan de registratie van: het

52 Zie ook *medicijn/hulpmiddel gebonden RFID*.

toedienen van medicijnen, het verstrekken van voeding en medische waarden zoals bloeddruk en pols.[53]
Uit het oogpunt van privacy en veiligheid is het opzetten van een één op één uitwisselingssysteem het overwegen waard. Bij een ziekenhuisopname geeft de patiënt zijn kaart in bewaring in ruil voor een polsbandje. Verwisseling van patiënten en hun gegevens zou dan theoretisch tot het verleden moeten behoren.
Een bewakingssysteem voor psychiatrische en geriatrische patiënten behoort eveneens tot de mogelijkheden van een polsbandje. Voor een goede traceermogelijkheid verdient het gebruik van een long-range passieve of actieve RFID-tag de voorkeur. Het traceren van personen ligt qua privacy erg gevoelig. Het moge duidelijk zijn dat deze traceermogelijkheid wordt toegepast in het belang van de patiënt zelf. Dit weegt mijns inziens dan ook ruimschoots op tegen de inbreuk op de privacy van de patiënt.

5.3.2 Implantaten

De RFID-tag leent zich, mede door zijn beperkte omvang, voor vele toepassingen als implantaat. Mogelijke toepassingsgebieden zijn identificatie en monitoring van zowel de implantaten als de patiënten. De toepassing als identificatiemiddel trekt de meeste aandacht van de media. Opmerkelijk is de relatieve stilte rondom het andere toepassingsgebied. Dit terrein omvat tamelijk uiteenlopende toepassingen, die in de nabije toekomst een behoorlijk grote impact kunnen hebben op de gezondheidszorg.

De RFID-tag als identificatie-implantaat
De meest voor de hand liggende toepassing van een RFID-implantaat is die als identificatiemiddel. Dit is dan ook gelijk de meest omstreden vorm. Duidelijk blijkt dat RFID groot is geworden in de logistieke identificatie. Dit heeft als gevolg dat het vraagstuk van de privacy een centrale rol krijgt toebedeeld, zodra een koppeling met personen, bijvoorbeeld via kleding, wordt gemaakt. De techniek van het tracken en tracen kan ook direct op mensen toegepast worden, waardoor de rol van de privacy nog evidenter wordt. Met betrekking tot de juridische discussie rondom de toepassing van RFID-technologie plaats ik de volgende kanttekeningen. Ze speelt zich nagenoeg geheel af op het terrein van de privacy. Fictie en feiten worden daar niet altijd even zuiver onderscheiden. Onbekendheid met de technologische (on)mogelijkheden speelt daarbij een aanzienlijke rol.

[53] Zie ook de toepassing van RFID-polsbandjes in het Akita University Hospital. (Akita, Japan), zoals beschreven in *Medicijn/hulpmiddel gebonden RFID*.

Men dient zich terdege bewust te zijn van de risico's die RFID-implantaten met zich mee kunnen brengen, maar zich ook te realiseren dat angst een slechte raadgever is. Een geïmplanteerde identificatietag is effectief[54] niets anders dan een tatoeage. Gezien de maatschappelijke gevoeligheid met betrekking tot privacy, lijkt het mij verstandig terughoudend te zijn met het louter implanteren van tags omwille van de identificatie.
Het implanteren van een tag raakt aan het grondrecht op bescherming van de lichamelijke integriteit (artikel 11 Grondwet). Het spreekt vanzelf dat het inbrengen van een RFID-implantaat enkel mag gebeuren met voorafgaande toestemming van de betrokkene. Wellicht zijn er in uitzonderlijke gevallen zwaarwegende redenen om geen toestemming te vragen aan de betrokkene (bijvoorbeeld het voor de eigen veiligheid taggen van handelingsonbekwame patiënten).

Commerciële toepassingen van RFID-implantaten zijn op dit moment nog beperkt in aantal. Het Amerikaanse Applied Digital levert de 11-millimeter lange VeriChip. Deze RFID-tag is voorzien van een uniek identificatienummer, waarmee men via een database alle persoonlijke gegevens van de betrokkene, zoals adres, telefoonnummer en speciale medische informatie kan achterhalen. De chip met het formaat van een rijstkorrel, kan door een huisarts met een spuit subdermaal onder de rechter triceps worden ingebracht. Doordat de tag alleen een unieke code bevat worden beveiligingsrisico's enigszins beperkt. Met betrekking tot privacy dient opgemerkt te worden dat de tag juist wordt gebruikt wanneer de drager zelf niet bij machte is zijn identiteit en kenmerken aan te geven (bijvoorbeeld wanneer de patiënt door een aanval bewusteloos is). In dergelijke gevallen zou de verwerkingsgrond artikel 8, onder d van de Wbp kunnen zijn.
Het identificatie-implantaat is niet de toepassingsvorm waarvan ik verwacht dat ze de grootste vlucht zal nemen. Deze rol lijkt mij weggelegd voor de meer gespecialiseerde monitoringstags. Tegen het monitoren van bepaalde functies van het menselijk lichaam zal maatschappelijk beduidend minder weerstand bestaan.

RFID als monitoringsimplantaat
In de nabije toekomst is een grote rol te verwachten van specialistische monitoringstags. Deze apparaatjes zullen voorzien zijn van een gespecialiseerd monitoringsdeel en een RFID-transmissiedeel. Ze kunnen generiek aangemaakt wor-

[54] Want, hoewel een geïmplanteerde tag niet zichtbaar hoeft te zijn, is deze functioneel vergelijkbaar met een streepjescode, een oormerk of een tatoeage.

den[55] en zullen bijvoorbeeld kunnen worden toegepast om patiënten met diabetes mellitus II ('ouderdomssuiker') in staat te stellen om 'contactloos', zonder te prikken, hun bloedsuikergehalte te meten.
Voor dergelijke veelvoorkomende aandoeningen kunnen dit soort medische voorzieningen rendabel worden geëxploiteerd. Omdat in dit soort toepassingen slechts één waarde wordt doorgegeven, kan worden gesteld dat er effectief geen sprake hoeft te zijn van identificatie. De meetgegevens hoeven dus niet per definitie persoonsgegevens te zijn, maar door spontane herkenning of koppeling aan andere gegevens kunnen ze dat wel gemakkelijk worden. Wanneer deze gegevens teruggevoerd kunnen worden op een identificeerbare natuurlijke persoon, is er sprake van bijzondere persoonsgegevens in de zin van paragraaf 2 van de Wbp. Immers, de meetgegevens zeggen iets over de gezondheid van de betrokkene. Vanuit juridisch oogpunt is het voornaamste aandachtspunt bij monitoringtags de verwerking van de verkregen meetgegevens.
In de praktijk zal het privacyprobleem in een dergelijke situatie marginaal zijn: alleen van zeer dichtbij kan men te weten komen of iemand een monitoringstag bij (of zo men wil: in) zich draagt, van buiten af is aanwezigheid van een implantaat niet waarneembaar en de verstrekte informatie is zeer beperkt.[56] Of dit door patiënten wordt ervaren als privacygevoelige informatie, kan men zich afvragen. Privacy is een beleving en de patiënt ervaart dat de lusten boven de lasten gaan.[57]
Voorbeelden van toepassingen voor dergelijke RFID-tags zijn het monitoren van de bloedglucose (zoals bij patiënten met diabetes mellitus) of het cardiovasculaire systeem. In de laatste categorie kan men denken aan het opnemen van de bloeddruk (hypo/hypertensie), de pols en hartfuncties. Het draadloos monitoren van volledig digitale pacemakers is al enige tijd mogelijk.

---

55 Met andere woorden, ze hoeven niet van een unieke code voorzien te worden die per definitie gekoppeld is aan een persoon. De verkregen meetgegevens zijn als zodanig niet noodzakelijkerwijs persoonsgegevens. Hoewel de meetgegevens op zichzelf geen persoonsgegevens hoeven te zijn zal de inrichting van het RFID-systeem meestal wel tot gevolg hebben dat de meetgegevens als persoonsgegevens beschouwd moeten worden.

56 Het is een momentopname uit een reeks, niet bedoeld om individueel opgeslagen te worden. Wel wordt vaak de tendens over een langere termijn genoteerd of opgeslagen in een (elektronisch) dossier. Deze informatie kan in een achterliggende database aan een identificeerbare natuurlijke persoon gekoppeld worden.

57 Er lopen ook mensen met een rollator, die zijn dus minder valide. Maar is dit realistisch gezien identificatie?

Een RFID-tag om op te eten
Het Japanse Animal Industry Lab in Takayama, Gifu Prefecture heeft een RFID-toepassing voor koeien ontwikkeld. Het betreft geen elektronisch oormerk, maar een chip die de gezondheid bewaakt. De beesten krijgen een speciale RFID-tag in hun maag. Deze is bewust groter dan normaal, zodat de tag niet uit de maag verdwijnt. Iedere keer als de koeien zich in de buurt van een meetpunt begeven, wordt hun lichaamstemperatuur gemeten. Het is tevens mogelijk ademhalingsritme, hartslag en, indien de koe zwanger is, gegevens over het kalf te meten.
Maar ook de mens slikt al omwille van zijn gezondheid een RFID-tag. Spelers van de Philadelphia Eagles, de Jacksonville Jaguars en de Minnesota Vikings (National Football League) slikken een 'Radio Pill' om hun lichaamstemperatuur te monitoren. Dit doen ze om oververhitting in een vroeg stadium te kunnen signaleren. Het apparaatje dat ze slikken is de Cortemp ingestible core body thermometer pill van HQ Inc. De pil biedt de mogelijkheid om ongeveer 24 uur lang de lichaamstemperatuur met behulp van een datarecorder te zenden naar een handheld apparaat. Daarna verlaat de pil op natuurlijk wijze het lichaam. Goedkoop is het niet: de kosten per team zijn zo'n $ 5.000-7.500 voor een setje pillen, twee of drie datarecorders en een handheld (PDA).

Naast deze toepassingen waarbij het monitoren met een korte interval plaatsvindt, zijn ook vele toepassingsmogelijkheden met een extensieve vorm van monitoren in de nabije toekomst realiseerbaar.
Op dit moment levert een Japanse fabrikant al schroeven die voorzien zijn van een High Frequency (13.56 MHz) RFID-tag. De tag zit in de bout en registreert het tijdstip waarop de schroef was bevestigd en het aanhaalmoment (de kracht) waarmee de schroef was aangedraaid.[58] In het verlengde van deze toepassing ligt de monitoring van de schroef gedurende de gehele levenscyclus. Deze RFID-technologie zou tevens op protheses kunnen worden toegepast. Voortbouwend op het pientere schroefje zullen tevens pientere protheses ontwikkeld worden. De kunstheup die aangeeft dat er sprake is van overbelasting of overmatige slijtage behoort dan tot de mogelijkheden. De vraag of deze RFID-tag tevens voor de, aan het implanteren, voorafgaande logistieke keten kan worden ingezet, moet (nu nog) ontkennend beantwoord worden. De logistieke keten is het meest gebaat bij RFID-systemen die werken volgens de huidige EPCglobal-standaarden. De RFID-systemen voor het monitoren van implantaten zullen het meest gebaat zijn bij het gebruik van lagere frequentiebanden en relatief beperkte signaalsterkte. Het gebruik van de lagere frequentiebanden resulteert over het algemeen in een

[58] Als backup zijn de identificatienummers van de RFID-tag met behulp van laser in de schroeven gegraveerd. Boeiend is dat Volvo Cars in Gent deze gegevens volledig RFID-loos vastlegt. Men meet, om dezelfde redenen, echter niet vanuit de schroef maar vanuit de 'sleutel'.

betere geleiding ten aanzien van vloeistoffen en metaal. Het verhoudingsgewijs zwakke signaal is op grond van gegevensbeveiliging en de fysieke veiligheid van personen te prefereren. Wellicht dat in de toekomst voor dergelijke systemen een nieuwe RFID-standaard wordt ontwikkeld.
De incompatabiliteit met de huidige EPCglobal-standaarden heeft ook nog juridische voordelen. Indien voor zowel de logistieke keten als het monitoren van het implantaat in het lichaam, dezelfde RFID-tag gebruikt zou worden, zou deze door het implanteren van een objectgebonden tag veranderen in een persoonsgebonden tag. Daarnaast zou het vervolggebruik van dezelfde tag een, uit het oogpunt van privacy, gevoelige situatie opleveren: de traceermogelijkheid van de tag, met specificaties volgens de EPCglobal-standaard, wordt door de drager overgenomen. Deze problematiek doet zich, ingeval men gebruikmaakt van twee afzonderlijke tags, niet voor.

De RFID-implantaten worden steeds kleiner en het is dan ook slechts een kwestie van tijd dat ze volledig onder de noemer van de medische nanotechnologie[59] vallen. Deze technologieën maken nieuwe behandelmethoden mogelijk. Het is het meest waarschijnlijk dat, in plaats van het creëren van een complete nieuwe regelgeving voor kleine technologische medische producten, Europese wetgevers deze producten, indien mogelijk, binnen de reikwijdte van bestaande regelgeving zullen onderbrengen.
Drie medische apparaatrichtlijnen zijn hier van belang. Dit zijn de Active Implantable Medical Device Directive (90/385/EEC), de Medical Device Directive (93/42/EEC) en de In Vitro Diagnostic Medical Device Directive (98/79/EC); alsook, in mindere mate de Medicinal Products Directive (2004/27/EC). Een potentieel probleem is dat geen van deze richtlijnen geschreven is met de nanotechnologie in gedachten. De Medical Device Directive (MDD) wordt bijvoorbeeld, als een 'new approach' richtlijn ondersteund door 'geharmoniseerde' Europese normen (de veiligheidsnormen voor elektrisch-medische apparatuur uit de IEC 60601-serie), die voorzien in een veronderstelling van overeenstemming met verschillende essentiële vereisten van de richtlijn. Deze standaarden bevatten een serie van biologische veiligheden (EN ISO 10993-series), hetgeen waarschijnlijk een volgend probleem oplevert bij producten die gebaseerd zijn op nanotechnologie. Geen van de biocompatibiliteitstesten in deze serie is ontworpen met het oog op de specifieke eigen-

[59] Dit is wetenschap op 'nano'niveau (in het algemeen beschouwd formaat tussen 1 nm en 100 nm). Het is niet nieuw of gerelateerd aan een bepaalde (sub)tak van wetenschap. Wat wel betrekkelijk nieuw is, is het exact manipuleren van materiaal op nanoschaal, hetgeen de creatie van nieuwe materiaaltypen en de miniaturisering van mechanismen en machines mogelijk maakt.

schappen van nanotechnologische producten. Herziening van ten minste enkele van de huidige harmonisatienormen zal dan ook nodig zijn. Bovendien zullen de essentiële vereisten van de richtlijnen moeten worden herzien om rekening te houden met specifieke risico's van RFID-nanotechonologische producten.[60]
In 2003 is de NEN-EN-ISO 13485 Kwaliteitsmanagement Medische Hulpmiddelen gepubliceerd. De norm is geschikt voor het ontwerp, de productie en de behandeling van medische hulpmiddelen. Een nieuwe norm was nodig omdat onder meer afstemmingsproblemen ontstaan waren met de nieuwe NEN-EN-ISO 9001:2000.[61] De Europese Richtlijn Medische Hulpmiddelen (Medical Device Directive: MDD) is opgenomen in de Nederlandse wetgeving door het Besluit medische hulpmiddelen.[62] Sinds april 2004 is de NEN-EN-ISO 13485 geregistreerd als geharmoniseerde norm. Dit betekent dat de norm in overeenstemming is met de drie Europese richtlijnen voor medische hulpmiddelen: MDD 93/42/EC (Medische hulpmiddelen), IVDD 98/79/EC (In vitro diagnostica) en AIMD 90/385/EC (Actieve implantaten).

5.4 Objectgebonden RFID-toepassingen

De toepassingsmogelijkheden van objectgebonden RFID-technologie in de zorgsector zijn ruim. Omdat de RFID-tag niet direct aan een persoon gekoppeld wordt, is deze categorie minder privacygevoelig dan persoonsgebonden toepassingen. De huidige discussie rondom het tracken en tracen[63] van goederen in de logistiek en detailhandel en het (vermeende) risico van schending van de privacy is wel één op één te kopiëren naar de zorgomgeving. Enige categorieën objectgebonden toepassingen worden hieronder nader beschreven. Het zijn de dossiergebonden RFID-toepassingen, RFID-toepassingen ten behoeve van medicatieverstrekking, kwaliteits- en echtheidscontrole van medicijnen en de specialistische logistieke keten voor medicijnen en hulpmiddelen. Aansluitend geef ik een korte

---

60 Een ander probleem is het grensoverschrijdend karakter van apparaten die nanotechnologie bevatten. Ik doel hier niet op grensoverschrijdend in de zin van grensverleggend, maar op grensoverschrijdend in de zin van vallend onder verschillende wet- en regelgeving. Meer en meer zullen we bij toepassing van (medische) nanotechnologie geconfronteerd worden met het hybride karakter van een product. Een RFID-implantaat bijvoorbeeld is niet alleen een zend- en ontvangsteenheid, maar tevens een implantaat en een medisch meetinstrument. Hybride producten zijn lastig bij één regeling onder te brengen.

61 Deze problemen vonden hun grondslag in twee belangrijke aspecten van de ISO 9001: continue verbetering en klanttevredenheid. Deze principes zijn geen vereisten onder de Richtlijn Medische Hulpmiddelen (Medical Device Directive).

62 Besluit van 30 maart 1995, houdende regels met betrekking tot het in de handel brengen en het toepassen van medische hulpmiddelen, alsmede tot wijziging van enige algemene maatregelen van bestuur.

63 Het tracken en tracen volgens de EPCglobal standaarden in de logistieke sector.

beschrijving van de huidige stand van zaken met betrekking tot de gewone logistieke processen in de zorg.

5.4.1 Dossiergebonden RFID

Als mogelijke toepassingen van dossiergebonden RFID kan men bijvoorbeeld denken aan de logistiek rondom het fysieke archief (als zuiver logistieke toepassing ter ondersteuning van het verkeer van de huidige papieren dossiers), beveiliging van toegangsmogelijkheden door personeel tot het fysieke archief en/of elektronische data met behulp van RFID-tags (bijvoorbeeld als vervanging van de kaarten met een magneetstrip), segmentatie in specialismen ten behoeve van de privacy van de patiënt (toewijzing door middel van een elektronische koppeling van specialismen aan een patiëntenkaart) en combinaties met EPD.[64] Verder spelen tevens de algemene vraagstukken van beveiliging en beheer van de patiëntengegevens.[65] In dit kader kan men opmerken dat er een onderscheid is tussen adaptatie van technologische en organisatorische beveiliging.[66] Aandacht op dit gebied verdient ook de voortdurende wijziging van de rollen van de verzekeraar, de huisarts, de specialist en de zorginstelling. Duidelijk is wel dat inmenging en de verantwoordelijkheid van de afdeling ICT aanzienlijk zal toenemen.
In augustus 2005 zijn twee belangrijke contracten op het gebied van elektronische uitwisseling van patiëntengegevens ondertekend. De ondertekenaars zijn enerzijds het Nationaal ICT Instituut in de Zorg (NICTIZ) en anderzijds de vertegenwoordigers van twaalf regio's in Nederland. Deze zogeheten twaalf koploperregio's zijn betrokken bij de ontwikkeling en invoering van een Elektronisch Medicatie Dossier (EMD) en een elektronisch waarneemdossier voor huisartsen (WDH). Het Ministerie van VWS hecht grote waarde aan een snelle landelijke invoering van deze digitale dossiers. In 2006 gaat de landelijke infrastructuur voor informatie-uitwisseling in de zorgsector van start met de invoering van het elektronisch medicatiedossier[67] en het elektronisch waarneemdossier huisartsen. Deze projecten vormen de eerste hoofdstukken van een volledig landelijk elektronisch patiëntendossier. De invoering van het EPD staat gepland voor 2010. Ontsluiting van deze informatie met behulp van RFID kan op eenzelfde wijze

---

64 Zie ook hiervoor *de patiëntenkaart* en over het EDP in het algemeen: <http://www.nictiz.nl/>

65 Een goed overzicht van de huidige stand van zaken geeft: Spaink, K., (2005), *Medische geheimen, risico's van het elektronisch patiëntendossier,* Amsterdam: Nijgh & van Ditmar.

66 Over het algemeen worden acties in deze richting door de afdeling ICT geïnitieerd. Vaak zijn dergelijke afdelingen technology-driven waardoor het bedrijf of de instelling qua ontwikkelingen op het organisatorische en juridische vlak achterblijft.

67 De beoogde invoering van het Elektronisch Medicatie Dossier staat gepland rond medio 2006.

geschieden als beschreven bij de toepassing van de patiëntenkaart. Een extra vorm van identificatie is hier raadzaam. Dit zou door middel van het hanteren van een pincode naast de kaart getackeld kunnen worden. Op dit moment is er nog geen specifieke wet- en regelgeving met betrekking tot RFID-toepassingen in de zorg. Met betrekking tot de dossiers zelf geldt dat op grond van de Wet bescherming persoonsgegevens en de veiligheidsnorm NEN 7510 een beveiligde en gecodeerde opslag verplicht is.

5.4.2 Medicijn/hulpmiddel gebonden RFID

Het meest voor de hand liggend is het traceren en lokaliseren van vitale medicatie. RFID-technologie kan een praktisch hulpmiddel zijn bij het op het juiste tijdstip en in de juiste hoeveelheden toedienen van medicijnen. Veelal zijn de verpakkingseenheden van medicijnen reeds voorzien van een label voor logistieke monitoring. Ik verwacht in eerste instantie toepassing bij langcyclische, dure medicijnen. Indien de prijs per tag verder zakt, staat tevens een massale toepassing bij logistieke verspreiding van andere medicijnen niets in de weg. De toepassingen kunnen bestaan uit het verlengen van de logistiek tracering tot aan het verpleegbed. Deze tracerings- en identificatiemogelijkheid hoeft natuurlijk niet te stoppen zodra de eindgebruiker de medicijnen verkrijgt. Het Akita University Hospital (Akita, Japan) heeft een behoorlijk vergaande variant, om medische missers tegen te gaan, ingevoerd. Dit RFID-systeem monitort alle mogelijke combinaties tussen verpleegkundige, medicijnen en patiënt.[68] Verdergaande toepassingen zoals het verplicht versturen van een 'kill' commando[69] na toediening als beveiliging, zijn naar mijn mening ook een optie. In een dergelijk geval dient de patiënt of verzorgende door een druk op een knop de toegediende eenheid te af te melden. Een minder vergaande vorm kan bestaan uit het attenderen van de patiënt op de noodzaak en het moment van toediening, waarbij na toediening het waarschuwingssignaal door afmelding van de tag stopt. Een boeiend project in deze context is de eerdergenoemde Parkinsonpas. Mensen met de ziekte van Parkinson gebruiken veel verschillende medicijnen, die vaak ook op verschillende tijdstippen moeten worden ingenomen. De pas kan functioneren als 'medicijnenwekker' en alarmeert de patiënt die vervolgens op de display van de bijgeleverde kaartlezer ziet welk medicijn op dat moment dient te worden ingenomen.[70] Vanuit het oogpunt van privacy zullen bij deze toepassing goede waarborgen gehan-

---

68 Zie ook hoofdstuk 2 en het gebruik van RFID-polsbandjes zoals beschreven bij *de patiëntenkaart*.

69 Zie Schermer, B.W. en Durinck, M., (2005), *Privacyrechtelijke aspecten van RFID*, p. 39-40, ECP.NL.

70 Zie hiervoor *de patiëntenkaart*.

teerd moeten worden, daar het gaat om de verwerking van bijzondere gegevens in de zin van paragraaf 2 van de Wbp.

5.4.3 Kwaliteits- en echtheidscontrole

Een andere mogelijke toepassing is de controle van de kwaliteit en echtheid van medicijnen en medische hulpmiddelen. Vooral dure medicijnen worden op grote schaal nagemaakt. Om gezondheidsrisico's te voorkomen, dient namaak te worden tegengegaan. In de strijd tegen namaakmedicijnen kan RFID een grote rol spelen. Afhankelijk van de kostprijs per eenheid, kan men de gehele zending, de colli, de verpakkingseenheid zoals de doosjes of het individuele medicijn van een tag voorzien en daarmee de echtheid en kwaliteit garanderen.[71]
Opmerkelijk is dat de mogelijkheden medicijnen met behulp van RFID-technologie te kunnen traceren en op echtheid te kunnen controleren unaniem bijval krijgen. Zelfs het als kritisch bekendstaande Bits of Freedom hanteert een ronduit mild standpunt in haar 'Dossier RFID en Privacy'.[72]

Pilot study Biomet
Methec heeft in samenwerking met SAP een pilot study uitgevoerd naar de mogelijkheden van RFID bij Biomet. Biomet is een leverancier van producten voor de musculoskeletale markt (kunstgewrichten). In dit soort omgevingen wordt veel gewerkt met leensets. Dit zijn dozen met alle implantaten en instrumenten die tijdens een operatie gebruikt kunnen worden. Slechts enkele implantaten worden tijdens de operatie verbruikt, de overige gaan terug naar de leverancier. Na terugkomst worden de leensets gecontroleerd, gescand en aangevuld. Tijdens de pilotstudy werd men geconfronteerd met de standaardcommunicatieproblemen tussen de reader en de RFID-tags, maar ook met, de meer specifieke, problemen zoals het bestand zijn van tags tegen een lange levenscyclus met veel te ondergane handelingen en Gammastraling (ten behoeve van sterilisatie).

Vanuit het oogpunt van privacy is het belangrijkste bij de toepassing van RFID in dit kader, dat er geen koppeling wordt gemaakt tussen patiënt en medicijn indien dit niet strikt noodzakelijk is. Wanneer er sprake is van 'item level tagging' bij medicatie ontstaat op het gebied van privacy eenzelfde discussie als in de detail-

71 Totdat een handige crimineel het voor elkaar krijgt de RFID-tags na te maken.
72 Verhaegh, S., (2004), *Dossier RFID en Privacy Bits of Freedom*.

handel, namelijk die van de koppeling tussen productinformatie en een natuurlijk persoon.[73]

5.4.4 De gewone logistieke processen in de zorg

Naast de specifiek aan de zorgsector gerelateerde toepassingen, is een zorginstelling dagelijks het terrein van een grote logistieke operatie. De RFID-toepassingen die men hier kan inzetten vallen binnen de reikwijdte van de standaardlogistieke toepassingen. Ze worden hier dan ook slechts kort beschreven.
De Nederlandse Vereniging van Ziekenhuizen (NVZ) en vereniging Logistiek management (vLm) zijn recent een samenwerking gestart. Deze samenwerking richt zich op het belang van goede logistiek in de gezondheidszorg. Initiatieven, die op dit gebied zijn gestart naar aanleiding van het TPG-rapport 'Sneller Beter', werden op 2 november 2005 tijdens het congres Zorglogistiek 'scan uw toekomst' gepresenteerd.[74] De NVZ presenteert tijdens dit congres de Quick Scan Zorglogistiek aan de Minister van Volksgezondheid, Welzijn en Sport. Deze scan biedt voor ziekenhuizen een handvat, waarmee stapsgewijs het organisatieproces in kaart kan worden gebracht en inzicht kan worden verkregen in de onderdelen die vanuit kwaliteits- en doelmatigheidsperspectief voor verbetering vatbaar zijn. Een aantal ziekenhuizen wordt momenteel in concrete logistieke projecten ondersteunt door TPG Post. Ook hebben NVZ en vLm samen een project zorglogistiek opgezet, waarvan dit najaar de eerste resultaten worden gepresenteerd. Bovendien hebben NVZ en vLm tijdens voormeld congres een intentieverklaring tot structurele samenwerking ondertekend. Daarmee wordt een logistieke ondersteuning en productontwikkeling voor alle ziekenhuizen op langere termijn beoogd.
De beschrijving van de juridische consequenties met betrekking tot de gewone logistieke processen komt uitgebreid elders in deze uitgave aan de orde.

5.5 Conclusie

De mogelijkheden van RFID-toepassingen in de gezondheidszorg zijn zeer ruim. RFID kan een katalysator voor (nog) meer efficiency en effectiviteit in de zorg worden. Beperkingen in toepasbaarheid van alternatieve technologieën zoals biometrie en barcodes, scheppen mogelijkheden voor de toepassing van RFID. De

---

[73] Zie hiervoor onder andere: Schermer, B.W., Durinck, M., (2005), *Privacyrechtelijke Aspecten van RFID*, ECP.NL mei 2005.

[74] *Sneller Beter – Logistiek in de Zorg*, Eindrapport TPG 17 juni 2004. Zie: <http://www.snellerbeter.nl>

RFID-systemen die werken op lagere frequentiebanden, genieten vanuit het oogpunt van veiligheid (beperking elektromagnetische interferentie) en beveiliging (proximity dus privacy) de voorkeur. Gezien de voor de zorg specifieke vereisten, is het wellicht raadzaam een speciale RFID-standaard voor de zorg te ontwikkelen. Te meer daar deze omgeving meer dan gemiddeld privacygevoelig is, is het van evident belang bij deze ontwikkeling de juridische impact en aspecten scherp voor ogen te hebben. Een complicerende factor hierbij is de nieuwheid van de materie. Op dit moment is er nog geen specifieke wet- en regelgeving met betrekking tot RFID-toepassingen in de zorg.

De juridische aspecten van RFID vormen zeker ook in zorgomgevingen een belangrijk aandachtspunt. Dit geldt met name voor privacygerelateerde vraagstukken. Zolang deze vraagstukken niet goed worden geadresseerd, zal invoering van RFID-technologie tot weerstand bij patiënten leiden. Indien de eigen gezondheid ermee gediend is, zijn patiënten of hun naasten geneigd (vermeende) privacygevoeligheden op de koop toe te nemen. In levensbedreigende situaties accepteert men zelfs ronduit snel inmenging in de privacy. Acceptatie door doorsnee patiënten vereist daarentegen een goed gevoel bij hen. Ze laten zich daarbij vaak leiden door emoties. Onder meer gevoed door de media, is angst hierbij vaak de raadgever. Het is aan de gezondheidszorg om, mede met behulp van goede voorlichting, deze angst weg te nemen. Of het wakende oog van Hippocrates daartoe toereikend is, staat te bezien.

6 Werknemers en RFID

Jessica Verwer

6.1 Inleiding

In de loop der jaren heeft de werkgever steeds meer methoden tot zijn beschikking gekregen om informatie over zijn werknemers te verzamelen. Door middel van het gebruik van personeelsvolgsystemen kan de aanwezigheid, het gedrag en de productiviteit van de werknemers worden geobserveerd, gemeten en geregistreerd.[75] Controle en toezicht door de werkgever zijn een onderdeel van een arbeidsrelatie. Tussen werkgever en werknemer heerst immers een gezagsrelatie. De werknemer kan zich echter wel jegens zijn werkgever beroepen op het recht op privacy en de werkgever dient zich te houden aan de eisen van goed werkgeverschap.[76]

RFID is een technologie die uitermate geschikt is voor het volgen van werknemers. Door het gebruik van RFID in een personeelsvolgsysteem kan de werkgever gemakkelijker en op veel grotere schaal gegevens over zijn werknemers verzamelen en verwerken in een database. De huidige toepassing van RFID beperkt zich (voornamelijk) tot toegangscontrolesystemen: door middel van een contactloze smart card in een badge, welke de werknemers verplicht als identificatiemiddel bij zich dienen te dragen, is het mogelijk de aankomst- en vertrektijden te registreren zonder dat er fysiek contact nodig is tussen de reader en de kaart. Het valt te verwachten dat op korte termijn de RFID-technologie op bredere schaal zal worden toegepast op de werkplek. De vraag is of de huidige regelgeving de werknemer voldoende waarborgen biedt voor de bescherming van zijn privacy bij het gebruik van RFID op de werkplek.

Teneinde deze vraag te beantwoorden wordt eerst het begrip personeelsvolgsystemen besproken. Tevens wordt daarbij gekeken wat het gebruik van RFID binnen een dergelijk systeem tot gevolg heeft. Vervolgens wordt ingegaan op het huidige juridische kader, te weten: de regels met betrekking tot het goed werkgeversschap, zoals verankerd in het Burgerlijk wetboek (BW), de Wet bescherming persoonsgegevens (Wbp) en de Wet op de ondernemingsraden (WOR). Daarna zal kort stil worden gestaan bij de Wet heimelijk cameratoezicht en de rechtsbe-

---

75 J.H.J. Terstegge, (2002), 'Privacy en werkplek' in *Privacyregulering in theorie en praktijk*, Deventer: Kluwer, p. 281.

76 Zie onder andere EHRM *Halford v. the United Kingdom*, judgment of 25 June 1997, *Reports* 1997-III, p.1016, § 45 en Hof 's-Hertogenbosch 2 juli 1986, *NJ* 1987, 451 (Koma/FNV).

scherming van de werknemers. Aansluitend volgen een conclusie en enige aanbevelingen

6.2 Personeelsvolgsystemen en RFID

Een personeelsvolgsysteem kan gedefinieerd worden als 'een doorgaans geautomatiseerd systeem waarin individuele en geaggregeerde gegevens van en over werknemers worden vastgelegd en dat als doel heeft (1) het ondersteunen van beslissingen ten aanzien van individuele werknemers en/of (2) het verschaffen van informatie met het oog op het voeren van een doelmatig en efficiënt personeelsbeleid en personeelsmanagement'.[77] Van belang is dat een dergelijk systeem systematisch raadpleegbaar is. De geautomatiseerde controle op het email- en internetgebruik van werknemers valt onder de term personeelsvolgsysteem. Maar ook het gebruik van toegangspasjes, camera's, of black boxes (rijtijden registratie in vrachtwagens) zijn vormen van personeelsvolgsystemen. Voor de vraag of een systeem als personeelsvolgsysteem moet worden aangemerkt, moet niet zozeer worden gekeken naar de gebruikte techniek, maar naar het doel in relatie tot het vastleggen en controleren van de aanwezigheid, gedrag of prestaties van de werknemers.
Het gebruik van RFID is op zichzelf nooit een personeelsvolgsysteem; het is slechts een techniek in een groter systeem. Het gebruik van RFID-technologie binnen een personeelsvolgsysteem vergemakkelijkt veelal het verzamelen en verwerken van gegevens over de werknemers. Het heeft echter niet tot gevolg dat er geheel andere informatie kan worden verzameld en verwerkt. Het gebruik van RFID brengt dan ook voornamelijk een kwalitatief verschil met zich mee.
Eveneens is van belang dat het verzamelen en verwerken van gegevens over de werknemers met behulp van RFID ook heimelijk kan plaatsvinden. Dit is echter met veel andere personeelsvolgsystemen ook al het geval: cameratoezicht kan heimelijk plaatsvinden en ook de controle op het email- en internet gebruik kan zonder dat de werknemer daarvan op de hoogte is plaatsvinden.
Het is echter niet uit te sluiten dat door het gebruik van RFID nieuwe volgsystemen mogelijk worden die nu nog niet bestaan. Men zou bijvoorbeeld kunnen denken aan 'active badge monitoring'. Door middel van elektronische ogen (RFID-readers) en badges met RFID-tags kunnen de werknemers door het hele gebouw worden gevolgd. Dit volgen door het gebouw is ook met camera's te rea-

[77] J.H.J. Terstegge, *Personeelsinformatiesystemen en privacybescherming*, te vinden op http://home.planet.nl/~privacy1/ pis2107.htm

liseren. Echter, met behulp van RFID kunnen de tijdstippen waarop de werknemer een bepaalde reader passeert direct worden opgeslagen in een achterliggende database.

6.3 Goed werkgeverschap

Binnen een arbeidsovereenkomst is er altijd sprake van een zekere machtsverhouding. Dit brengt bepaalde beperkingen van de grondrechten van de werknemer met zich mee. De Registratiekamer, de voorganger van het College bescherming persoonsgegevens, heeft dit als volgt geformuleerd:

> *In werktijd geniet men niet dezelfde vrijheden als daarbuiten. De arbeidsverhouding brengt zekere beperkingen met zich mee voor de grondrechten van werknemers. Tegenover het loon staat de verplichting werkzaamheden te verrichten onder het gezag van de werkgever en hierbij diens aanwijzingen op te volgen. De werknemer is als gevolg daarvan in meer of mindere mate beperkt in zijn bewegings- en handelingsvrijheid en in zijn vrijheid van meningsuiting. Hetzelfde geldt voor zijn recht op privacy. Met het betreden van de werkplaats moet de werknemer een deel van zijn aanspraken op respect voor zijn persoonlijke levenssfeer inleveren. Dit betekent niet dat een werkgever bij het nastreven van zijn belang zonder meer aan de belangen en fundamentele vrijheden van zijn medewerkers voorbij kan gaan.*[78]

Er zijn dus grenzen aan de controlebevoegdheid van de werkgever en de belangrijkste grens wordt gevormd door de inbreuk die een dergelijke controle op de persoonlijke levenssfeer van de werknemer maakt.
De bescherming van het privacyrecht van werknemers is binnen arbeidsverhoudingen onderdeel van de algemene norm van het ‘goed werkgeverschap’ dat is vastgelegd in artikel 7:611 BW. Dit artikel verplicht de werkgever zich te gedragen als een goed werkgever. Hiervan is geen sprake als zonder noodzaak of gerechtvaardigd belang dan wel met onevenredige middelen inbreuk wordt gemaakt op de persoonlijke levenssfeer van werknemers. Evenmin is er geen sprake van goed werkgeverschap als niet voldoende zorgvuldigheid wordt betracht bij het beoordelen van individuele werknemers op basis van de op de een of andere manier verzamelde gegevens over deze werknemers. Voorzover het gaat om het verzamelen van gegevens geldt als uitgangspunt, dat een werknemer zich moet kunnen verdedigen indien er bezwaren zijn tegen zijn functioneren. En

---

78 L.J.M. Dullaart, *Internet-Policies, controlebevoegdheid versus privacy,* Leiden: 2001, te vinden op www.xs4all.nl/~ljm/scriptie

daarvoor is essentieel dat hij weet op grond van welke feiten en omstandigheden hij wordt beoordeeld.[79]
Als het gaat om privacy komt, ook bij de beoordeling of er sprake is van goed werkgeverschap, uiteraard betekenis toe aan artikel 10 van de Grondwet (GW). In dit artikel is het recht op eerbiediging en bescherming van de persoonlijke levenssfeer vastgelegd.

> *Artikel 10 GW*
> *Ieder heeft, behoudens bij of krachtens de wet te stellen beperkingen, recht op eerbiediging van zijn persoonlijke levenssfeer. De wet stelt regels ter bescherming van de persoonlijke levenssfeer in verband met het vastleggen en verstrekken van persoonsgegevens. De wet stelt regels inzake de uitspraken van personen op kennisneming van over hen vastgelegde gegevens en van het gebruik dat daarvan wordt gemaakt, als mede op verbetering van zodanige gegevens.*

Artikel 8 van het Europees Verdrag voor de Rechten van de Mens (EVRM) biedt een soortgelijke bescherming:

> *Artikel 8 EVRM*
> *Een ieder heeft recht op respect voor zijn privéleven, zijn familie- en gezinsleven, zijn woning en zijn correspondentie. Geen inmenging van enig openbaar gezag is toegestaan in de uitoefening van dit recht, dan voor zover bij wet is voorzien en in een democratische samenleving noodzakelijk is in het belang van de nationale veiligheid, de openbare veiligheid of het economisch welzijn van het land, het voorkomen van wanordelijkheden en strafbare feiten, de bescherming van de gezondheid of goede zeden of voor de bescherming van de rechten en vrijheden van anderen.*

In het Edamse bijstandsmoeder-arrest heeft de Hoge Raad geoordeeld dat burgers, en dus ook werknemers, rechtstreeks een beroep kunnen doen op artikel 8 EVRM.[80]

6.4 Wet bescherming persoonsgegevens

De beginselen omtrent de omgang met persoonsgegevens zijn vastgelegd in de Wet bescherming persoonsgegevens (Wbp). De Wbp regelt zowel het verzamelen van persoonsgegevens als de omgang met persoonsgegevens.[81] Om van een persoonsgegeven te kunnen spreken moet de persoon op wie het gegeven betrekking heeft identificeerbaar zijn. Een persoon is identificeerbaar indien de identiteit van

---

79 J.H.J. Terstegge, (2002), *Goed werken in netwerken, Regels voor controle op e-mail en internetgebruik van werknemers* (Tweede herziene druk), Den Haag: College Bescherming Persoonsgegevens, p. 21.

80 HR 9 januari 1987, *NJ* 1987, 928, m.nt. E.A.A. (Edamse bijstandsmoeder).

81 J.H.J. Terstegge, (2002), *Privacy en werkplek* in 'Privacyregulering in theorie en praktijk', Deventer: Kluwer, p. 291.

de persoon redelijkerwijs, zonder onevenredige inspanning, is vast te stellen aan de hand van de gegevens die over deze persoon beschikbaar zijn. Er moet dus een direct of indirect verband zijn tussen de persoon en het gegeven.[82] Of een persoon, direct of indirect, identificeerbaar is wordt mede bepaald door de vraag of de verantwoordelijke feitelijk redelijkerwijs in staat is de identiteit van een persoon vast te stellen. Daarbij wordt gekeken naar de middelen die de verantwoordelijke (degene die zeggenschap heeft over de wijze waarop de gegevens worden verwerkt) kan of zal inzetten om een persoon te identificeren. In concrete gevallen moet onder andere rekening worden gehouden met bijzondere expertise en technische faciliteiten van de verantwoordelijke.[83]
Op grond van de Wbp kan de informatie die wordt verkregen door middel van een RFID-tag persoonsgegevens betreffen indien en voorzover die informatie betrekking heeft op een geïdentificeerde of identificeerbare persoon. Bij het gebruik van RFID binnen een personeelsvolgsysteem is er vaak sprake van het verwerken van persoonsgegevens. Immers, met een personeelsvolgsysteem worden in de regel gegevens van en over individuele werknemers verzameld en verwerkt. Het gebruik van een personeelsvolgsysteem moet derhalve voldoen aan de vereisten van de Wbp.

Voor het rechtmatig verwerken en het zorgvuldig en behoorlijk omgaan met persoonsgegevens schrijft de Wbp een aantal normen voor. Deze normen kunnen worden uitgewerkt naar de volgende basisvoorwaarden:
– *Doelbinding*. Persoonsgegevens worden voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden verzameld. Persoonsgegevens worden niet verder verwerkt op een wijze die onverenigbaar is met de doeleinden van de verkrijging (artikelen 7 en 9 Wbp).
– *Rechtmatige grondslag*. Er bestaat een rechtmatige grondslag voor het verzamelen van persoonsgegevens (artikel 8 Wbp).
– *Kwaliteit*. Gegevensverwerking dient in overeenstemming te zijn met de wet en behoorlijk en zorgvuldig te gebeuren (artikel 6 Wbp).
– *Transparantie*. De betrokkene moet kunnen overzien door wie en voor welk doel zijn gegevens worden verwerkt (met name de artikelen 33 t/m 35 Wbp).
– *Meldplicht*. De verwerking van persoonsgegevens dient vooraf te worden gemeld bij het College bescherming persoonsgegevens. Er kan een vrijstelling gelden (artikelen 27 t/m 30 Wbp).

---

82 B.W. Schermer & M. Durinck, (2005), *Privacyrechtelijke aspecten van RFID*, Krimpen aan den IJssel: Efficiënta Offsetdrukkerij, p. 23.
83 *Kamerstukken II* 1997-1998, 25 892, nr. 3, p. 49.

– *Beveiliging*. Er dienen passende maatregelen van technische en organisatorische aard te worden getroffen ter beveiliging van de persoonsgegevens (artikelen 12 t/m 14 Wbp).
– *Bewerker*. Indien de verantwoordelijke persoonsgegevens te zijnen behoeve laat verwerken door een bewerker, dan draagt hij zorg dat deze voldoende waarborgen biedt ten aanzien van de technische en organisatorische beveiligingsmaatregelen met betrekking tot de te verrichten verwerkingen (artikel 14 Wbp).

Zoals gezegd, heeft de werkgever een meldplicht, indien hij voornemens is met behulp van RFID persoonsgegevens over zijn werknemers te verzamelen en op te slaan. Deze melding heeft tot doel de transparantie van de gegevensverwerking te bevorderen[84] en maakt dat de afweging van de belangen van verantwoordelijke en betrokkenen tot op zekere hoogte inzichtelijk en controleerbaar zijn.
Op grond van artikel 29 Wbp kunnen minder risicovolle verwerkingen worden vrijgesteld van de meldplicht. Dit is gebeurt in het Vrijstellingsbesluit (Vb). Voor de werkgever-werknemerverhoudingen is vooral artikel 7 Vb van belang. Daarin staat de vrijstelling voor verwerkingen in het kader van de personeelsadministratie betreffende personen in dienst van of werkzaam ten behoeve van de verantwoordelijke, voorzover de verwerking slechts geschiedt voor (onder andere) de interne controle en de bedrijfsbeveiliging. Van deze vrijstelling kan evenwel alleen gebruik worden gemaakt als er een betrekkelijk beperkt aantal soorten van gegevens worden verzameld en verwerkt. Als gevolg daarvan zal een personeelsvolgsysteem niet snel vallen onder de vrijstelling, zodat het zal moeten worden gemeld bij het College bescherming persoonsgegevens.

Naast verplichtingen voor de werkgever bevat de Wbp rechten voor de werknemer. Zo heeft de werknemer het recht zich vrijelijk en met redelijke tussenpozen tot de verantwoordelijke te wenden met het verzoek hem mede te delen of hem betreffende persoonsgegevens worden verwerkt (artikel 35 Wbp). Daarnaast heeft de werknemer het recht om gegevens te verbeteren, aan te vullen, te verwijderen of af te schermen indien deze feitelijk onjuist zijn, voor het doel of de doeleinden van de verwerking onvolledig of niet ter zake dienend zijn dan wel anderszins in strijd met een wettelijk voorschrift worden verwerkt (artikel 36 Wbp). De werknemer kan verder, in verband met bijzondere persoonlijke omstandigheden, verzet aantekenen tegen de verwerking van gegevens op grond

84 *Kamerstukken II* 1997-1998, 25 892, nr. 3 (MvT).

van artikel 8, onder e en f Wbp (artikel 40 Wbp). Tevens kan de werknemer niet worden onderworpen aan een besluit waaraan voor hem rechtsgevolgen zijn verbonden of dat hem in aanmerkelijke mate treft, indien dat besluit alleen wordt genomen op grond van een geautomatiseerde verwerking van persoonsgegevens bestemd om een beeld te krijgen van bepaalde aspecten van zijn persoonlijkheid (artikel 42 Wbp). Het heimelijk gebruik van een personeelsvolgsysteem is in beginsel niet zonder voorafgaand onderzoek en toestemming van het CBP toegestaan (vergelijk artikel 32, eerste en tweede lid, jo. artikel 31, eerste lid, onder b, Wbp, alsmede artikel 34 jo. 43 Wbp).[85]

6.5 Wet op de ondernemingsraden

Op grond van de WOR heeft de ondernemingsraad een instemmingsrecht met betrekking tot het besluit van de werkgever om gebruik te maken van een personeelsvolgsysteem. Artikel 27, eerste lid, sub l, WOR omschrijft het als volgt:

> *Artikel 27, eerste lid, onder 1, WOR*
> *De ondernemer behoeft de instemming van de ondernemingsraad voor elk door hem voorgenomen besluit tot vaststelling, wijziging of intrekking van:*
> *l een regeling inzake voorzieningen die gericht zijn op of geschikt zijn voor waarneming van of controle op aanwezigheid, gedrag of prestaties van de in de onderneming werkzame personen;*
> *[] een en ander voor zover betrekking hebbende op alle of een groep van de in de onderneming werkzame personen.*

Alle voorzieningen die gericht zijn op of geschikt zijn voor waarneming van of controle op aanwezigheid, gedrag of prestaties van de werknemers vallen onder het instemmingsrecht. Derhalve is het al voldoende dat het systeem geschikt is als personeelsvolgsysteem; het hoeft niet daadwerkelijk als zodanig te functioneren.

Als de ondernemingsraad zijn instemmingsrecht uitoefent, betekent dit dat hij het besluit om gebruik te maken van een personeelsvolgsysteem onder andere moet toetsen aan de Wbp. Op grond van de WOR wordt dan dus vooraf gecontroleerd of het personeelsvolgsysteem voldoet aan de vereisten van de Wbp. In het tweede en zesde lid van artikel 27 WOR is bepaald hoe de instemmingsprocedure dient te verlopen. Van belang is dat wanneer de ondernemer (dat is degene die door de

[85] Zie voor een uitgebreidere bespreking van de Wbp de bijdrage van Peter Blok in hoofdstuk 4.

wet wordt geadresseerd) de instemming van de ondernemingsraad niet verkrijgt, hij drie opties heeft: (1) hij kan van zijn voorgenomen besluit afzien, (2) hij kan het voorgenomen besluit volgens de inzichten van de ondernemingsraad wijzigen, of (3) hij kan de kantonrechter toestemming vragen het besluit te nemen. Dit laatste kan de ondernemer niet alleen doen wanneer de ondernemingsraad een uitdrukkelijke beslissing neemt dat hij niet met het voorgenomen besluit kan instemmen, maar ook wanneer de ondernemingsraad nalaat binnen een redelijke termijn een beslissing omtrent het al dan niet verlenen van instemming te nemen.[86] Een besluit waarop de ondernemer niet de vereiste instemming van de ondernemingsraad of de toestemming van de kantonrechter heeft verkregen, is in beginsel nietig. De ondernemingsraad moet dan wel binnen de gestelde termijn van één maand, schriftelijk, een beroep hebben gedaan op deze nietigheid.
Opmerking verdient dat onder de werking van artikel 27 WOR alleen besluiten van algemene strekking vallen. Mocht een werkgever in het zeer uitzonderlijke geval besluiten bijvoorbeeld *badge monitoring* alleen toe te passen op één bepaalde werknemer, dat valt dit besluit niet onder het instemmingsrecht van de ondernemingsraad (maar uiteraard wel onder de Wbp).

Volledigheidshalve wordt gewezen op een wetsvoorstel met betrekking tot de medezeggenschap van werknemers. De regering wil de kwaliteit van de medezeggenschap verbeteren door meer maatwerk mogelijk te maken en de regelgeving eenvoudiger en toegankelijker te maken.[87] De WOR wordt daartoe vervangen door de Wet medezeggenschap werknemers,[88] dit omdat de WOR naar de mening van de regering inmiddels door verschillende veranderingsrondes te ingewikkeld en te ontoegankelijk is geworden.[89] Het wetsvoorstel is momenteel in behandeling bij de Tweede Kamer.

6.6 Wet heimelijk cameratoezicht

Voor de volledigheid zij hier gewezen op de Wet heimelijk cameratoezicht. Deze wet stelt het heimelijk maken van opnamen van personen in zowel openbare als besloten plaatsen strafbaar. Met de invoering van deze wet zijn de artikelen 139f

86 F.W.H. Vink, *Inzicht in de ondernemingsraad, Een toelichting bij de Wet op de ondernemingsraden*, Den Haag: Sdu Uitgevers 2005, p. 145.
87 *Kamerstukken II* 2004-05, 29 818, nr. 3 (MvT).
88 *Kamerstukken II* 2004-05, 29 818, nr. 2 (Voorstel van Wet).
89 *Kamerstukken II* 2004-05, 29 818, nr. 3 (MvT).

en 441b van het Wetboek van Strafrecht aangepast. Werkgevers kunnen onder de wet gebruik blijven maken van een verborgen camera mits zij daartoe een gerechtvaardigd belang hebben, de werknemers vooraf op duidelijke wijze zijn gewezen op de mogelijke inzet van verborgen camera's en de werkgever zich houdt aan de Wet op de ondernemingsraden.[90]
De Wet heimelijk cameratoezicht ziet op het heimelijk verzamelen van informatie. In die zin vertoont het te verdedigen rechtsbelang veel overeenkomsten met het rechtsbelang bij het gebruik van RFID op de werkplek. Deze wet heeft mijns inziens echter geen invloed op het gebruik van RFID op de werkplek daar het gebruik van RFID niet leidt tot het opnemen en vastleggen van beelden. De wet spreekt duidelijk van beelden en opnamen. Derhalve kan deze niet naar analogie worden toegepast op het gebruik van RFID. Wel is het zo dat juist de wijze waarop privacy van werknemers door de wetgever in het Wetboek van Strafrecht wordt beschermd, ook voor RFID een mogelijkheid biedt. Heimelijke waarneming door middel van camera's, heimelijk afluisteren van telefoongesprekken voorzover de werkgever daar geen belang bij heeft, *enzovoort* is strafbaar. Heimelijk gebruik van RFID met als doel het volgen van personeel zou dus op dezelfde wijze strafbaar kunnen worden gesteld.

6.7 Rechtsmiddelen

Het is gebruikelijk dat wanneer een werknemer een klacht heeft aangaande de werkgever, hij de klacht in eerste instantie intern voorlegt aan bijvoorbeeld de vertrouwenspersoon binnen de onderneming. Wanneer dat niet tot een bevredigende oplossing leidt, kan hij zijn klacht voorleggen aan de burgerlijke rechter op grond van artikel 7:611 BW. Ook kan de werknemer bij de burgerlijke rechter rechtstreeks een beroep doen op artikel 8 EVRM. Indien de werkgever zich bij het gebruik van RFID op de werkplek niet houdt aan de Wbp, dan kan de werknemer zijn klacht voorleggen aan het College bescherming persoonsgegevens, dat zich onder andere bezighoudt met bemiddeling en klachtafhandeling. Uiteraard kan de werknemer zich ook tot de burgerlijke rechter wenden.
Op grond van de WOR behoeft de werkgever instemming van de ondernemingsraad om voor het besluit om van een personeelsvolgsysteem gebruik te maken. Als de ondernemingsraad deze instemming niet geeft, kan de werkgever in plaats daarvan ook toestemming vragen van de kantonrechter, die deze zal geven als de

[90] Eerste Kamer, vergaderjaar 2002-2003, 27 732, nr. 57c (MvA).

weigering van de ondernemingsraad onredelijk is. Zonder instemming van de ondernemingsraad of de kantonrechter is het besluit nietig. Van belang is dan dat de ondernemingsraad de kantonrechter zou kunnen verzoeken om de werkgever te verplichten zich te onthouden van handelingen die strekken tot uitvoering of toepassing van het nietige besluit. Omgekeerd kan ook de werkgever de rechter verzoeken om te verklaren dat de ondernemingsraad ten onrechte een beroep doet op de nietigheid van het besluit.

6.8 RFID en de privacy van werknemers

RFID is een technologie die uitermate geschikt is voor het volgen van werknemers. Het voornaamste verschil tussen de huidige systemen en een systeem dat gebruikmaakt van RFID is gelegen in de hoeveelheid gegevens die automatisch kunnen worden verzameld en het gemak waarmee de gegevens vervolgens kunnen worden opgeslagen en verwerkt. Bovendien functioneert RFID contactloos en op afstand, waardoor de mogelijkheden tot het heimelijk verzamelen van gegevens toenemen. Daarnaast zijn er veel mogelijkheden om een systeem dat gebruikmaakt van RFID aan andere systemen te koppelen. Een goed voorbeeld van een dergelijke koppeling is de toepassing van RFID door Tesco. Omdat scheermesjes tot de drie meest gestolen artikelen in een supermarkt behoren, voorzag Gillette, in samenwerking met supermarktketen Tesco, de scheermesjes van RFID-tags. Het schap waar de mesjes lagen was uitgerust met een reader. Zodra er meer dan de gebruikelijke hoeveelheid scheermesjes uit het schap werd gepakt, werd dit met behulp van de tags en de reader geregistreerd. Vervolgens werden deze gegevens gekoppeld aan een camerasysteem. Dit had tot gevolg dat, zodra er scheermesjes uit het schap werden gepakt, er een video-opname werd gemaakt van de potentiële dief.
De hoeveelheid gegevens die kunnen worden verzameld, de mogelijkheid tot het heimelijk verzamelen van gegevens en de mogelijkheid tot het koppelen van systemen, maken dat het gebruik van RFID op de werkplek van invloed is op de privacy van werknemers. Het gebruik van RFID op de werkplek kan op verschillende aspecten van het begrip privacy betrekking hebben. Ten eerste kan het betrekking hebben op de privacy in algemene zin of de persoonlijke levenssfeer. Het recht op bescherming van de persoonlijke levenssfeer is vastgelegd in de Grondwet en in een aantal verdragen. Wanneer een werknemer van mening is dat zijn recht op eerbiediging van de persoonlijke levenssfeer is geschonden, dan kan hij rechtstreeks een beroep doen op artikel 8 EVRM. Ook heeft de werknemer de mogelijkheid een beroep te doen op artikel 7:611 BW. Bij de beoordeling of er

sprake is van strijd met het goed werkgeverschap moet de rechter artikel 10 Gw of artikel 8 EVRM meewegen.
Een tweede aspect van privacy waar het gebruik van RFID-technologie betrekking op kan hebben is het beginsel van behoorlijk gegevensbeheer. Dit wordt ook wel in verband gebracht met het recht op informationele privacy. Onder het recht op informationele privacy wordt verstaan het recht te beslissen over het verzamelen, opslaan en verstrekken van informatie over privé-gegevens, met inbegrip van een inzagerecht in de opgeslagen gegevens.[91] Dit aspect van het recht op privacy is nader uitgewerkt in de Wet bescherming persoonsgegevens. In het geval dat een werkgever RFID inzet op de werkplek, dan gebeurt dit in nagenoeg alle gevallen binnen een personeelsvolgsysteem. Het gebruik van een personeelsvolgsysteem heeft het verwerken van persoonsgegevens tot gevolg en dient derhalve getoetst te worden aan de Wbp.

Op grond van de WOR heeft de ondernemingsraad een instemmingsrecht met betrekking tot besluiten betreffende het inzetten van personeelsvolgsystemen. De ondernemingsraad dient een dergelijk besluit te toetsen aan de Wbp. In organisaties waar geen OR is, moet het personeel in elk geval worden voorgelicht over het gebruik dat kan worden gemaakt van personeelsinformatiesystemen. (De mogelijkheid tot) het gebruik van dergelijke systemen kan eventueel worden vastgelegd in het arbeidscontract.
Uit (onder andere) het transparantiebeginsel van de Wbp vloeit impliciet voort dat het heimelijk gebruikmaken van RFID op de werkplek in beginsel niet is toegestaan. Bovendien zal het heimelijk gebruikmaken van RFID al snel in strijd zijn met het goed werkgeverschap van artikel 7:611 BW. Om deze reden lijkt een equivalent van de Wet heimelijk cameratoezicht voor het gebruik van RFID niet nodig.

6.9 Conclusie

Een op de werkplek reeds veel gebruikte toepassing van RFID vindt men terug in toegangscontrolesystemen. Deze systemen dienen de veiligheid, maar kunnen ook worden toegepast ter controle van de werknemers. Hoewel toepassing op bredere schaal op het ogenblik nog niet echt aan de orde is, ligt het voor de hand dat RFID – al dan niet gekoppeld aan telecommunicatietoepassingen of GPS – op

[91] L. Strikwerda, conclusie bij het arrest van de Hoge Raad van 31 mei 2002 (LJN: AD9609, Hoge Raad, C00/247HR).

(korte) termijn veelvuldig zal worden ingezet bij het controleren van werknemers, ofwel in personeelsvolgsystemen. Dit betekent dat persoonsgegevens over de werknemers gemakkelijk op veel grotere schaal dan daarvoor kunnen worden verzameld en opgeslagen. Daarmee staat vast dat het gebruik van RFID op de werkplek ingrijpende gevolgen zal hebben voor de privacy van de werknemer.
De vraag is dan of de wet voldoende bescherming biedt tegen te vergaande inbreuken op de privacy van werknemers. In het voorgaande is uiteengezet dat dat inderdaad het geval is. Toch lijkt het verstandig om voor het gebruik van RFID nadere invulling te geven aan de voorwaarden van de Wbp, door middel van gedragscodes, waarin de normen van de Wbp worden uitgewerkt voor het gebruik van RFID op de werkplek. Vergelijkbare uitwerkingen zijn door verschillende organisaties en instanties opgesteld voor de controle op het email- en internetgebruik van werknemers. Uit de jurisprudentie blijkt dat de aanwezigheid van een dergelijke code wordt meegewogen in de beoordeling van het geschil. Het ligt voor de hand dat dit ook het geval zal zijn bij de controle van werknemers met behulp van RFID.

7 Criminaliteit en RFID

Bart Schermer

7.1 Inleiding

Het valt te verwachten dat RFID in de (nabije) toekomst een wezenlijk onderdeel gaat vormen van onze informatie- en communicatie-infrastructuur. Hoewel RFID in belangrijke mate zal gaan bijdragen aan onze welvaart en veiligheid zijn er, net als bij elke andere technologie, ook risico's zoals de mogelijkheid tot misbruik. In dit hoofdstuk zal daarom gekeken worden met welke vormen van RFID-misbruik we rekening moeten houden en hoe we dit misbruik strafrechtelijk kunnen kwalificeren.
Onder misbruik van RFID versta ik het aanwenden van RFID-technologie voor criminele doeleinden, het (pogen te) vernielen of ontregelen van RFID-systemen en het misbruiken van RFID-gegevens. Een scherp onderscheid tussen de verschillende soorten misbruik zal ik verder niet maken daar de verschillende soorten misbruik veel overlap vertonen. Een goed voorbeeld is het wederrechtelijk uitlezen van een RFID-tag, de daarop vastgelegde informatie kopiëren naar een valse RFID-tag en deze gebruiken om een transactie te doen. Hierbij is er zowel sprake van misbruik van een RFID-systeem, misbruik van RFID-gegevens, alsmede het gebruik van RFID voor criminele doeleinden.
Ik zal in dit hoofdstuk inventariseren in hoeverre misbruik van RFID past binnen ons huidige materiële strafrecht. Het is hiervoor allereerst van belang om vast te stellen of RFID een geautomatiseerd werk in de zin van de wet is. De reden hiervoor is dat veel mogelijke verschijningsvormen van het misbruik van RFID overeenkomsten vertonen met een aantal delictsomschrijvingen waarin de term 'geautomatiseerd werk' is opgenomen. De wettelijke definitie van een geautomatiseerd werk is te vinden in artikel 80sexies Sr:

> *Artikel 80sexies Sr*
> *Onder geautomatiseerd werk wordt verstaan een inrichting die bestemd is om langs elektronische weg gegevens op te slaan en te verwerken.*

Naar mijn mening lijdt het geen twijfel dat RFID-systemen alsmede de daaraan gekoppelde achterliggende ICT-infrastructuren als 'geautomatiseerde werken' in de zin van artikel 80sexies Sr beschouwd moeten worden. In de Memorie van Toelichting bij de Wet Computercriminaliteit I worden computers, netwerken van computers en geautomatiseerde inrichtingen voor telecommunicatie als voorbeelden van geautomatiseerde werken gegeven. Simpele elektronische apparaten die

niet met hun omgeving communiceren zoals bijvoorbeeld een elektronisch klokje vallen buiten de definitie.[92] Hoewel gediscussieerd kan worden of een RFID-tag op zichzelf een geautomatiseerd werk is, ben ik van mening dat, zeker in samenhang met de achterliggende ICT-infrastructuur, RFID-tags als geautomatiseerde werken gezien moeten worden daar zij bestemd zijn om langs elektronische weg gegevens op te slaan en te verwerken.
Daarmee zijn diverse bepalingen uit het Wetboek van Strafrecht mogelijk van toepassing op het misbruik van RFID. Ook de aanpassingen aan het Wetboek van Strafrecht die voort gaan vloeien uit het wetsvoorstel Computercriminaliteit II dienen in ogenschouw te worden genomen.[93] Het wetsvoorstel Computercriminaliteit dateert uit 1998 maar heeft door verschillende oorzaken ernstige vertraging opgelopen en is dus nog niet aangenomen. In maart 2005 werd het wetsvoorstel alsnog in gewijzigde vorm toegezonden aan de Tweede Kamer waar het inmiddels is aangenomen. Het wetsvoorstel lag ten tijde van het ter perse gaan van deze publicatie bij de Eerste Kamer.[94]

Nu een RFID-systeem als een geautomatiseerd werk valt te beschouwen is de volgende stap de strafrechtelijke kwalificatie van de verschillende soorten misbruik van RFID. Hierbij dient allereerst rekening te worden gehouden met de diverse onderdelen waaruit een RFID-systeem (over het algemeen) bestaat. De reden hiervoor is dat een aanval op het ene deel van een RFID-systeem strafrechtelijk een andere gedraging kan zijn dan een aanval gericht tegen een ander onderdeel van hetzelfde systeem. In hoofdstuk 2 is de technische inrichting van RFID-systemen reeds aan de orde geweest. Dit technische onderscheid dient als basis voor een verdeling die strafrechtelijk gezien relevant is. Ik zal bij de bespreking van de verschillende soorten RFID-misbruik het volgende onderscheid hanteren:
– RFID-tag
– RFID-signalen (de dataoverdracht tussen tag en reader)
– RFID-reader
– achterliggende ICT-infrastructuur.

Voor de meeste vormen van RFID-misbruik geldt dat de mogelijkheden ertoe worden gedicteerd door de gebruikte technologie, de gekozen beveiligingsmaatregelen en de manier waarop met de toepassing wordt omgegaan. Bij de bespre-

92 *Kamerstukken II* 1989-90, 21 551, nr. 3, p. 6.
93 *Kamerstukken II* 1998-1999, 26 671, nummers 1 en 2.
94 Zie voor een overzicht: <http://www.ejure.nl>

king van mogelijk RFID-misbruik ga ik dan ook veelal uit van 'worst case scenario's'. Dit heeft niet tot doel paniek te zaaien, maar door uit te gaan van worst case scenario's kunnen ook minder voor de handliggende verschijningsvormen van RFID-misbruik mee worden genomen in de juridische analyse.
Gezien de beperkte ruimte moet een analyse van het mogelijk misbruik van RFID enigszins algemeen blijven. Het is echter van belang te blijven beseffen dat RFID een verzamelnaam is voor een veelvoud aan (mogelijke) toepassingen. Zo valt er een onderscheid te maken tussen productgebonden toepassingen zoals de EPC-smartlabels en persoonsgebonden toepassingen zoals de OV-chipkaart. Deze verschillende toepassingen maken gebruik van verschillende soorten RFID-technologie. Dit heeft ook tot gevolg dat de diverse toepassingen verschillende kwetsbaarheden hebben. Daarnaast kent iedere RFID-technologie zijn eigen beveiligingen en beschermingsmechanismen. Bij het bespreken van de manieren waarop RFID misbruikt zou kunnen worden is het dus van belang in het achterhoofd te houden dat niet elke vorm van RFID-misbruik zomaar altijd mogelijk is, maar dat de mogelijkheden tot misbruik afhangen van de concrete RFID-implementatie.

7.2 Skimming

Skimming is het ongeoorloofd uitlezen van RFID-tags. Omdat RFID gebruikmaakt van radiosignalen is het eenvoudig om van een afstand heimelijk (onbeveiligde of slecht beveiligde) RFID-tags met een reader uit te lezen. Skimming is veelal een noodzakelijke eerste stap om andere, meer uitgebreide en schadelijke vormen van misbruik zoals *cloning* mogelijk te maken.
Een groot deel van de RFID-tags die in de toekomst gebruikt zullen worden, met name de EPC smart labels, zullen geen beveiligings- of authenticatiemechanismen hebben. Met andere woorden, deze tags zullen hun aanwezigheid en inhoud automatisch prijsgeven aan een compatibele reader. Het uitlezen van dergelijke tags is naar mijn mening géén gedraging die binnen het huidige strafrecht valt.
Ik ben van mening dat het uitlezen van onbeveiligde tags ook niet per definitie strafbaar gesteld moet worden.[95] De voornaamste reden is dat het handhaven van

[95] Het kan bepleit worden dat het uitlezen van een tag onder het bereik van artikel 139c Sr valt (het afluisteren van telecommunicatie, zie volgende paragraaf), immers er wordt een radiosignaal opgevangen. Ik heb ervoor gekozen dit niet te doen, omdat voordat het signaal opgevangen kan worden een handeling vereist is, namelijk het raadplegen van de tag door de reader. Hiermee is de communicatie dus gericht aan (en daarmee bestemd voor) de partij die het originele radiosignaal uitstuurde. De ratio achter artikel 139c Sr is dat er communicatie wordt opgevangen door een derde die geen partij is bij de communicatie en waarvoor het signaal niet bestemd is. Bij skimming kan dit niet gezegd worden.

een dergelijke bepaling gezien de werking van RFID (tags maken zichzelf automatisch bekend bij een reader) nagenoeg onmogelijk is. Het zou betekenen dat iedere eigenaar van een RFID-reader die per ongeluk het signaal oppikt van een onbeveiligde tag welke geen onderdeel (meer) is van het systeem waartoe de reader behoort, strafrechtelijk vervolgd kan worden. Het moge duidelijk zijn dat dit geen werkbare oplossing is.
Toch zijn er tal van scenario's te bedenken waarbij een verbod op het uitlezen van tags wenselijk is. Een mogelijke reden om het ongeoorloofd uitlezen van RFID wél strafbaar te stellen zou bijvoorbeeld het voorkomen van roofovervallen kunnen zijn. Een overvaller zou met behulp van een draagbare RFID-reader kunnen kijken welke personen dure spullen bij zich dragen om op basis hiervan zijn slachtoffer uit te kiezen. Het voorhanden hebben van een draagbare reader zou wellicht een strafbare voorbereidingshandeling kunnen constitueren (artikel 46 Sr). Artikel 46, eerste lid, Sr luidt:

> *Artikel 46*
> *1 Voorbereiding van een misdrijf waarop naar de wettelijke omschrijving een gevangenisstraf van acht jaren of meer is gesteld is strafbaar, wanneer de dader opzettelijk voorwerpen, stoffen, informatiedragers, ruimten of vervoermiddelen kennelijk bestemd tot het begaan van dat misdrijf verwerft, vervaardigt, invoert, doorvoert, uitvoert of voorhanden heeft.*

Maar het bewijzen van een strafbare voorbereidingshandeling in het kader van RFID is een lastige aangelegenheid. Want wanneer is het voorhanden hebben van een RFID-reader kennelijk bestemd tot het begaan van een misdrijf en wanneer niet? Het enkele bezit van een RFID-reader is naar mijn mening onvoldoende om te kunnen spreken van een strafbare voorbereidingshandeling. Zelfs het met een RFID-reader in een winkelstraat lopen is niet noodzakelijkerwijs de voorbode van een overval.
De mogelijkheid die overblijft is het creëren van een nieuw artikel in het Wetboek van Strafrecht. Wanneer wij een strafrechtelijk verbod op het uitlezen van RFID willen invoeren dan zullen in de delictsomschrijving in ieder geval de bestanddelen 'opzettelijk' en 'wederrechtelijk' opgenomen moeten worden om te voorkomen dat het per ongeluk uitlezen van RFID-tags automatisch een strafbaar feit constitueert. Naast het strafbaar stellen van skimming moet ook gekeken worden welke technische oplossingen voorhanden zijn om skimming te voorkomen (beveiliging, kooi van Faraday).
Wanneer een crimineel een *beveiligde* RFID-tag wil uitlezen, dan zal hij de beveiliging door middel van een hack moeten omzeilen.[96] Hacking, oftewel computervredebreuk is strafbaar gesteld in artikel 138a Sr. In het wetsvoorstel Computercriminaliteit II wordt de maximale strafmaat voor hacking verhoogd en zijn

enkele tekstuele wijzigingen doorgevoerd. Om deze reden worden hier de eerste twee leden van artikel 138a Sr geciteerd, zoals zij in het wetsvoorstel zijn opgenomen:

Artikel 138a

1 Met gevangenisstraf van ten hoogste een jaar of geldboete van de vierde categorie wordt, als schuldig aan computervredebreuk, gestraft hij die opzettelijk en wederrechtelijk binnendringt in een geautomatiseerd werk of in een deel daarvan. Van binnendringen is in ieder geval sprake indien de toegang tot het werk wordt verworven:

a door het doorbreken van een beveiliging,

b door een technische ingreep,

c met behulp van valse signalen of een valse sleutel, of

d door het aannemen van een valse hoedanigheid.

2 Met gevangenisstraf van ten hoogste vier jaren of geldboete van de vierde categorie wordt gestraft computervredebreuk, indien de dader vervolgens gegevens die zijn opgeslagen in een geautomatiseerd werk waarin hij zich wederrechtelijk bevindt, overneemt en voor zichzelf of een ander vastlegt.

In tegenstelling tot onbeveiligde RFID-tags is het dus niet toegestaan beveiligde RFID-tags ongeoorloofd uit te lezen omdat hiervoor een beveiliging doorbroken moet worden of anderszins een technische ingreep moet worden gedaan.

7.3 Opvangen RFID-signaal

Het wederrechtelijk opvangen van een RFID-signaal kan gezien worden als een vorm van afluisteren c.q. aftappen. Als de wederrechtelijk verkregen gegevens ook nog vastgelegd worden, dan is er sprake van het opnemen van gegevens. In artikel 139c, eerste lid, Sr is het afluisteren, aftappen en opnemen van gegevens strafbaar gesteld:

Artikel 139c

1 Met gevangenisstraf van ten hoogste een jaar of geldboete van de vierde categorie wordt gestraft hij die opzettelijk en wederrechtelijk met een technisch hulpmiddel gegevens aftapt of opneemt die niet voor hem bestemd zijn en die worden verwerkt of overgedragen door middel van telecommunicatie of door middel van een geautomatiseerd werk.

Maar het is maar de vraag of het opvangen van een RFID-signaal strafbaar is op grond van artikel 139c Sr. Getuige de redactie van artikel 139c, tweede lid, Sr

[96] Uiteraard kunnen ook de achterliggende ICT-systemen die bij een RFID-toepassing horen gehacked worden, ook in dit geval is er sprake van computervredebreuk.

(afluisteren van telecommunicatie) lijkt het erop dat het afluisteren van een RFID-signaal *an sich* niet strafbaar is:

> *Artikel 139c*
> *2 Het eerste lid is niet van toepassing op het aftappen of opnemen:*
> *1 van door middel van een radio-ontvangapparaat ontvangen gegevens, tenzij om de ontvangst mogelijk te maken een bijzondere inspanning is geleverd of een niet toegestane ontvanginrichting is gebruikt.*
> *2 door of in opdracht van de gerechtigde tot een voor de telecommunicatie gebezigde aansluiting, behoudens in geval van kennelijk misbruik;*
> *3 ten behoeve van de goede werking van een openbaar telecommunicatienetwerk, ten behoeve van de strafvordering, dan wel ter uitvoering van de Wet op de inlichtingen- en veiligheidsdiensten 2002.*

Getuige de tekst van artikel 139c, tweede lid, onder 1, Sr is het artikel niet van toepassing op door middel van een radio-ontvangapparaat ontvangen gegevens. Een RFID-reader kan naast zenden, ook radiosignalen ontvangen en past daarmee binnen de definitie van een radio-ontvangapparaat. De ratio achter 139c, tweede lid, onder 1, Sr is dat de ether in principe vrij is, oftewel signalen die door de ether gaan genieten niet direct strafrechtelijke bescherming, tenzij voor het opvangen ervan een bijzondere inspanning is geleverd.[97] Een bijzondere inspanning is getuige de Memorie van Toelichting bij de Wet Computercriminaliteit I bijvoorbeeld het koppelen van verschillende radio-ontvangapparaten om daar vervolgens stelselmatig mee af te luisteren.[98]
Dit leidt ons tot de conclusie dat wanneer er wel opzettelijk gegevens worden getapt en/of opgenomen, maar er geen bijzondere inspanning hoeft te worden geleverd om de gegevens te achterhalen (bijvoorbeeld omdat het signaal onversleuteld is), het opvangen van de gegevens niet strafbaar is. Een en ander doet in het kader van RFID vreemd aan omdat een gedraging gericht op het verkrijgen van gegevens vastgelegd in de RFID-tag wél strafbaar is als de aanval gericht is op de beveiligde RFID-tag zelf, maar niet strafbaar wanneer de aanval is gericht op de overdracht van onversleutelde gegevens die na het authenticatieproces worden verzonden! Ook de in het wetsvoorstel Computercriminaliteit II voorgestelde redactie van het nieuwe artikel 139c Sr verandert niets aan deze situatie, daar artikel 139c, tweede lid, onder 1, Sr ongewijzigd blijft.

---

97 *Kamerstukken II* 1989-1990, 21 551, nr. 3, p. 18-19. Zie ook: T.J. Noyon, G.E. Langemeijer, J. Remmelink, (2000), *Het Wetboek van Strafrecht*, 7e druk, voortgezet door J.W. Fokkens en A.J. Machielse, p. 235; en Wedzinga, (2002), (*T&C Strafrecht*) artikel 139c Sr, aant. 9.
98 *Kamerstukken II* 1989-1990, 21 551, nr. 3, p. 19.

Een aanpassing van de wet lijkt dus voor de hand te liggen. Wanneer de wetgever echter wil vast blijven houden aan het principe van de vrije ether, dan is het zaak gebruikers van RFID voor te lichten over de wenselijkheid van het ten alle tijden versleutelen van gegevens.

7.4 Wijzigen en/of wissen van RFID-gegevens

Wanneer een RFID-tag 'read/write' functionaliteit heeft, is het mogelijk om de inhoud van de tag te wijzigen. Dit opent voor criminelen de mogelijkheid om de op de tag vastgelegde informatie te veranderen of te wissen.[99] Naast de mogelijkheid om RFID-gegevens op de tag zelf te veranderen bestaat er ook de mogelijkheid om gegevens te wijzigen of te wissen welke zijn opgeslagen in de achterliggende ICT-systemen die bij de RFID-toepassing horen.
Strafrechtelijk valt het wederrechtelijk veranderen, wissen, onbruikbaar of ontoegankelijk maken van RFID-gegevens (zowel op de tag, als in het achterliggende ICT-systeem) binnen de huidige delictsomschrijving van artikel 350a, eerste lid, Sr, alsmede binnen de delictsomschrijving zoals die is voorgesteld in het wetsvoorstel Computercriminaliteit II:

> *Artikel 350a*
> *1 Hij die opzettelijk en wederrechtelijk gegevens die door middel van een geautomatiseerd werk <u>of door middel van telecommunicatie</u> zijn opgeslagen, worden verwerkt of overgedragen, verandert, wist, onbruikbaar of ontoegankelijk maakt, dan wel andere gegevens daaraan toevoegt, wordt gestraft met gevangenisstraf van ten hoogste twee jaren of geldboete van de vierde categorie.*[100]

7.5 Cloning

Naast het wijzigen van RFID-data is het ook mogelijk om RFID-tags te 'klonen'. Dit houdt in dat de informatie van een RFID-tag gekopieerd wordt naar een andere tag of gegevensdrager die daarmee identiek wordt aan het origineel. Met een gekloonde RFID-tag zijn allerlei vormen van misbruik mogelijk. Het is hier

---

99 Hierbij past de kanttekening dat herschrijfbare RFID-tags over het algemeen ook beter beveiligd zijn. Dit betekent dat een crimineel eerst de beveiliging zal moeten omzeilen alvorens hij de op de tag vastgelegde gegevens kan wijzigen of wissen.

100 De aanpassing zoals voorgesteld in het wetsvoorstel Computercriminaliteit II is onderstreept.

zinvol een onderscheid te maken tussen productgebonden RFID-tags en persoonsgebonden RFID-tags.
Het klonen van productgebonden RFID-tags opent met name de mogelijkheid tot diefstal en tot namaak. Bij persoonsgebonden RFID-tags (zoals bijvoorbeeld een betaalpas, OV-chipkaart of biometrisch paspoort) valt met name te denken aan delicten zoals fraude, identiteitsdiefstal en andere vormen van oplichting (artikel 326 Sr).
Hoewel de voor cloning veelal noodzakelijke gedragingen, computervredebreuk (artikel 138a Sr), het wederrechtelijk afluisteren en vastleggen van gegevens (artikel 139c, tweede lid, Sr) en het voorhanden hebben van een voorwerp met daarop wederrechtelijk verkregen gegevens (artikel 139e Sr), reeds op zichzelf staande delicten zijn, zal een gekloonde tag veelal een hulpmiddel vormen bij zwaardere delicten zoals oplichting welke met een zwaarder strafmaximum bedreigd zijn.

7.6 RFID denial of service attack

Wanneer in de toekomst steeds meer processen, voorzieningen en diensten afhankelijk worden van RFID-technologie, dan kan het voor criminelen (of vandalen) interessant worden om deze diensten te ontregelen.
Een methode om RFID-systemen te ontregelen is de RFID denial of service attack (DoS). Het doel van een denial of service attack is om een geautomatiseerd werk met een dusdanige hoeveelheid informatieverzoeken en/of waardeloze data te bestoken dat het geautomatiseerde werk de dienst die het verleent moet staken. Een denial of service attack is een veel gebruikte aanval op het internet. Een bekend voorbeeld is de verstoorde chatsessie van Willem Alexander en Máxima met het Nederlandse publiek in 2002. De chatsessie moest onderbroken worden omdat een groep hackers de chatservers onklaar wist te maken met behulp van een grootschalige denial of service attack.
Een denial of service attack zou bijvoorbeeld in een supermarkt tot grote chaos kunnen leiden. Zou je vroeger met een zwarte viltstift de supermarkt in moeten stappen om alle barcodes zwart te stiften, nu volstaat het uitschakelen/onbruikbaar maken van de RFID-readers om in een mum van tijd chaos te veroorzaken. Onderzoek is vereist naar de mogelijkheden en de gevolgen van het onklaar maken van RFID-readers bij de verschillende toepassingen.
Momenteel kan een denial of service attack al naar gelang hoe de gedraging concreet plaatsheeft onder verschillende artikelen worden geschaard. Een denial of service attack past momenteel binnen de reikwijdte van de artikelen 350a Sr,

161sexies Sr of 161septies Sr. Denial of service attacks worden in het wetsvoorstel Computercriminaliteit II echter apart strafbaar gesteld:

> *Artikel 138b*
> *Met gevangenisstraf van ten hoogste een jaar of geldboete van de vierde categorie wordt gestraft hij die opzettelijk en wederrechtelijk de toegang tot of het gebruik van een geautomatiseerd werk belemmert door daaraan gegevens aan te bieden of toe te zenden.*

Oorspronkelijk bevatte het voorgestelde artikel een zinsnede die het bereik van het artikel beperkte tot een denial of service aanval verricht via een openbaar telecommunicatienetwerk, echter deze zinsnede komt in het meest recente voorstel niet meer voor. Door de nieuwe, techniekonafhankelijke redactie van het artikel kan ook een RFID denial of service attack onder het bereik van de bepaling worden gebracht.

7.7 Vernieling van een RFID-systeem

Naast het ontregelen van een RFID-systeem door middel van een denial of service attack of een hack, bestaat ook de mogelijkheid tot het fysiek vernielen van een RFID-systeem. Hierbij kan uiteraard gedacht worden aan het handmatig vernielen of onklaar maken van RFID-readers of tags, maar het vernielen van een RFID-systeem met behulp van krachtige elektromagnetische straling (EMP) of een ontlading van statische elektriciteit (ESD) vormt een potentieel grotere dreiging. Een elektromagnetische puls of een ontlading van statische elektriciteit kan in theorie alle RFID-apparaten (met name tags) die zich binnen de straal van de puls of de ontlading bevinden onbruikbaar maken. Diensten die (in de toekomst) afhankelijk zijn van RFID kunnen hierdoor ernstig ontregeld worden. Op internet wordt al volop gediscussieerd over draagbare EMP- en ESD-apparaten en andere manieren om de delicate circuits van een RFID-tag uit te schakelen.[101] Er is weinig fantasie voor nodig om in te beelden welk effect het gebruik van deze apparaten zou kunnen hebben in de toekomst op een supermarkt of het openbaar vervoer. Het vernielen van een RFID-systeem past binnen de delictsomschrijving van artikel 161sexies Sr dan wel van artikel 161septies Sr. Daarnaast zouden ook de artikelen 350 Sr en artikel 350a Sr van toepassing kunnen zijn.

[101] Zie bijvoorbeeld www.indymedia.nl en www.securityfocus.com

7.8 Tracking en hotlisting

Een belangrijke toepassing van RFID-technologie binnen de logistiek is het tracken en tracen van goederen. Uiteraard kunnen dergelijke toepassingen van RFID-technologie ook door criminelen worden gebruikt. Criminelen zouden bijvoorbeeld zelf RFID-systemen kunnen inzetten om de locatie van waardevolle goederen te achterhalen, of andermans RFID-systemen hacken om te achterhalen wat de locatie van bepaalde goederen is.
RFID kan ook ingezet worden voor (bedrijfs)spionage. Informatie over de goederenstromen, voorraden en producten van de concurrent kan bijzonder waardevol zijn. Door het op uitgebreide schaal uitlezen van RFID-tags en het afluisteren van radiosignalen kan dergelijke informatie boven water worden gehaald.
Bij de hierboven genoemde gedragingen is RFID duidelijk een hulpmiddel en hoewel het misbruik van RFID hier misschien als zelfstandig strafbaar feit vervolgd zou kunnen worden, zal de uiteindelijke handeling (bedrijfsspionage, diefstal) van groter belang zijn. Het tracken en tracen van goederen zal wederom als strafbare voorbereidingshandeling of begin van uitvoering gezien kunnen worden, al naar gelang de aard van het feit waarvoor de RFID-systemen of -gegevens worden gebruikt. In het geval van de bedrijfsspionage zal uit de opgevangen en vastgelegde gegevens meestal snel blijken dat het om bedrijfsspionage gaat.

Naast goederen kunnen ook mensen worden gevolgd en/of gelokaliseerd met behulp van (actieve) RFID-tags. Ook deze toepassing van RFID zou door criminelen misbruikt kunnen worden. Het is mogelijk dat criminelen hun doelen ongemerkt uitrusten met (actieve) RFID-tags (het 'taggen' van een persoon). Criminelen kunnen ook de reeds door het doelwit gebruikte tags aanwenden. Hiervoor zijn de persoonsgebonden RFID-tags (zoals die in OV-kaarten, bankpassen, of paspoorten) uiteraard het meest interessant, maar ook een unieke 'constellatie' van door de persoon gedragen tags kan als identificerend middel gebruikt worden. Hierbij moet gedacht worden aan combinaties van tags in onder andere kleding, schoenen en horloges.
Criminelen kunnen allerlei redenen hebben voor het volgen van personen. Qua gedraging heeft het volgen van een persoon met behulp van RFID nog het meest weg van het delict belaging (artikel 285b Sr), in de volksmond beter bekend als stalking. Het eerste lid van het artikel luidt als volgt:

Artikel 285b

1 Hij, die wederrechterlijk stelselmatig opzettelijk inbreuk maakt op eens anders persoonlijke levenssfeer met het oogmerk die ander te dwingen iets te doen, niet te doen of te dulden dan wel vrees aan te jagen wordt, als schuldig aan belaging, gestraft met een gevangenisstraf van ten hoogste drie jaren of een geldboete van de vierde categorie.

We zien dat het eerste gedeelte van het eerste lid: '*… Hij, die wederrechterlijk stelselmatig opzettelijk inbreuk maakt op eens anders persoonlijke levenssfeer…*' in het kader van het iemand heimelijk met een RFID-tag uitrusten van toepassing zou kunnen zijn. Waar het echter spaak loopt is het tweede deel van het eerste lid: '*… met het oogmerk die ander te dwingen iets te doen, niet te doen of te dulden dan wel vrees aan te jagen wordt'*. Wanneer criminelen RFID in zouden zetten zal dit nagenoeg altijd heimelijk gebeuren, doel van de toepassing is volgen, niet dreigen. Aldus zal artikel 285b Sr niet van toepassing zijn op het heimelijk taggen van personen omdat een bestanddeel van de delictsomschrijving niet bewezen kan worden. Het taggen van een persoon zal over het algemeen de opmaat vormen voor een strafbaar feit (bijvoorbeeld beroving, ontvoering of moord). Het heimelijk taggen van een persoon zou dus als het begin van de uitvoering van een strafbaar feit kunnen worden gezien. Maar hier lopen wij tegen het probleem aan dat het onduidelijk is om welk strafbaar feit het zal gaan waarmee het bewijzen ervan uiteraard moeilijk wordt. Het voorhanden hebben van (actieve) tags om personen te taggen zou ook een strafbare voorbereidingshandeling kunnen zijn. Maar net als bij RFID-readers is het voorhanden hebben van tags met de opzet om deze kennelijk te gebruiken voor een strafbaar feit moeilijk te bewijzen.
De vraag rijst dus of het heimelijk taggen van een persoon een zelfstandig strafbaar feit zou moeten constitueren, daar het sterke inbreuk op de persoonlijke levenssfeer kan opleveren. Momenteel bestaat er in het Wetboek van Strafrecht geen verbod op het heimelijk volgen van een persoon met behulp van een technisch hulpmiddel, daar tot op heden geen noodzaak was voor een dergelijk artikel. De stand van de techniek maakt het nu echter mogelijk om iemand heimelijk uit te rusten met een RFID-tag waardoor deze persoon (makkelijker) gevolgd kan worden.

We zien dat de ontwikkeling van nieuwe technologiën (computers, camera's) vaak aanleiding is voor de wetgever om het strafrecht aan te passen. Het meest recente voorbeeld is de Wet heimelijk cameratoezicht die op 1 januari 2004 in werking is getreden.[102] De Wet heimelijk cameratoezicht betreft een wijziging van de artikelen 139f Sr en 441b Sr. Het is met ingang van 1 januari 2004 verboden om zonder hen hiervan op de hoogte te brengen met behulp van (vaste) camera's personen te filmen.[103] Het is dus niet zozeer verboden om toezicht te

[102] Wet van 8 mei 2003 tot wijziging van de artikelen 139f en 441b van het Wetboek van Strafrecht (uitbreiding strafbaarstelling heimelijk cameratoezicht), *Stb*. 2003, 198 Strafrecht (uitbreiding strafbaarstelling heimelijk cameratoezicht), *Stb*. 2003, 198.

[103] Het filmen van personen in openbare ruimtes met behulp van een handcamera is niet strafbaar, daar er geen sprake is van een 'aangebracht technisch hulpmiddel', waardoor een bewezenverklaring van het feit onmogelijk wordt.

houden op personen voor bijvoorbeeld beveiligingsdoeleinden, maar wel om dit heimelijk te doen. Artikel 139f luidt als volgt:

> *Artikel 139f*
> *Met gevangenisstraf van ten hoogste zes maanden of geldboete van de vierde categorie wordt gestraft:*
> *1 hij die, gebruik makende van een technisch hulpmiddel waarvan de aanwezigheid niet op duidelijke wijze kenbaar is gemaakt, opzettelijk en wederrechtelijk van een persoon, aanwezig in een woning of op een andere niet voor het publiek toegankelijke plaats, een afbeelding vervaardigt;*
> *2 hij die de beschikking heeft over een afbeelding welke, naar hij weet of redelijkerwijs moet vermoeden, door of ten gevolge van een onder 1 strafbaar gestelde handel*

Omdat de wet specifiek ziet op cameragebruik is deze in het kader van RFID niet toepasbaar. Maar het bedreigde rechtsgoed van de burger (dat van zijn privacy) is gelijk, om deze reden lijkt een vergelijkbaar artikel (liefst technologie onafhankelijk) het overwegen waard.
Naast het volgen van personen houdt de unieke identificatie van personen nog een aanvullende dreiging in, te weten die van het zogenoemde 'hotlisting'. Hotlisting betekent dat de unieke identificatie van een persoon gebruikt wordt om een bepaalde gebeurtenis wel of niet plaats te laten vinden. Zo kan een hotlist met daarop identificatienummers bijvoorbeeld gebruikt worden om voetbalsupporters met een stadionverbod de toegang tot het stadion te ontzeggen. Maar een hotlist kan ook door criminelen of terroristen worden gebruikt als startsein voor bijvoorbeeld een bomaanslag. Wanneer het doelwit (een minister, rechter, of gewoon burgers van een bepaald land) voorbij een (draagbare) reader loopt vormt de 'match' met de hotlist de 'trigger' om de bom af te laten gaan. Specifiek om deze reden is in de Verenigde Staten hevig protest uitgebroken tegen het voornemen van de federale overheid om onbeveiligde RFID-tags in paspoorten te gebruiken.[104]

7.9 Conclusie

Onze maatschappij wordt in steeds hogere mate afhankelijk van informatie- en communicatietechnologie. Zo zijn telefonie en internet nu al onmisbare kritieke infrastructuren voor Nederland.[105] Gezien de huidige ontwikkelingen zal RFID

[104] www.wired.com/news/privacy/0,1848,67333,00.html
[105] Zie onder andere beleidsnota Kwetsbaarheid Internet (KWINT). *Kamerstukken II* 2000-01, 26 643, nr. 30.

ook in de toekomst een onderdeel van onze kritieke informatie- en communicatie-infrastructuur gaan worden. Het wordt dan ook voor criminelen steeds interessanter om RFID te gebruiken en te misbruiken.
In dit hoofdstuk zijn diverse vormen van mogelijk RFID-misbruik geïnventariseerd. Over het algemeen lijkt het Wetboek van Strafrecht alsmede de daarop voorgestelde aanpassingen door de techniekonafhankelijke redactie redelijk goed te gebruiken in het kader van RFID. Belangrijke uitzonderingen worden echter gevormd door het uitlezen van onbeveiligde tags (geen strafbepaling) en het afluisteren van onbeveiligde RFID-signalen (de uitzondering van artikel 139c, tweede lid, onder 1, Sr).
Een specifiek probleem betreft voorts de inzet van RFID als hulpmiddel bij andere strafbare feiten (diefstal, spionage, beroving, ontvoering, moord). In een aantal gevallen zou het voorhanden hebben van RFID-apparatuur een strafbare voorbereidingshandeling kunnen opleveren en het gebruik ervan een begin van uitvoering. Het bewijs van zoiets dergelijks is echter geen makkelijke zaak. Zo is het voorhanden hebben van een draagbare RFID-reader niet noodzakelijkerwijs een strafbare voorbereidingshandeling, net zo min als dat het rondlopen met een dergelijke reader in een winkelstraat een begin van uitvoering van een strafbaar feit is. Verder is het heimelijk volgen van personen met behulp van RFID géén zelfstandige strafbare gedraging, maar zal dit wel een inbreuk op de privacy zijn.

Nu wij aan de vooravond staan van een grootscheepse implementatie van RFID is het zaak dat we de mogelijke risico's ervan goed in kaart brengen. Ik ben van mening dat het niet de technologie zelf, maar de uiteindelijke toepassing ervan is die bepaalt welke (maatschappelijke) gevaren er al dan niet kunnen ontstaan. Om risico's tot een minimum te beperken is het dus zaak om de technologie op een verantwoorde manier in te zetten. Bij de bouw en het gebruik van RFID-systemen moet daarom, net als bij elke andere technologie, rekening worden gehouden met de mogelijkheden die het biedt voor misbruik.
Waar nodig moet dan gezocht worden naar oplossingen die liggen op het vlak van beveiliging, voorlichting maar ook wet- en regelgeving. Hierbij moet strafrecht altijd *ultimum remedium* blijven. Het is daarom ook belangrijk te beseffen dat RFID als technologie slechts de draadloze overdracht van informatie tussen twee punten bewerkstelligt. Als zodanig moet bij de strafrechtelijke kwalificatie van misbruik van RFID goed gekeken worden welk deel van een RFID-systeem nu daadwerkelijk het doelwit is van misbruik. Veelal zal dit niet de RFID-tag, RFID-signalen of de RFID-reader betreffen, maar de achterliggende databases. In deze gevallen gaat het dus niet zozeer om nieuwe strafbare gedragingen, maar om 'gewone' computercriminaliteit. Voor die gevallen waarbij RFID een nieuwe,

unieke situatie oplevert is plaats voor strafbaarstelling van genoemde gedragingen.

8 Internationale ontwikkelingen

Jeroen Koëter

8.1 Inleiding

De ontwikkeling van RFID en het EPCglobal Network wordt wereldwijd kritisch gevolgd door consumenten- en burgerrechtenorganisaties. De negatieve gevolgen die RFID kan hebben voor onze privacy en het feit dat bestaande wet- en regelgeving niet overal in de wereld toereikend lijkt, wordt inmiddels ook door marktpartijen erkend. De roep om regulering heeft in de Verenigde Staten al in twaalf deelstaten geleid tot voorstellen voor specifieke RFID-wetgeving. Hierna wordt een aantal van deze voorstellen beschreven. Ook zal blijken dat de meeste Europese landen veel minder haast maken met het reguleren van RFID. Naast overheidsregulering is een aantal marktpartijen ook gestart met (pogingen tot) zelfregulering. In dit hoofdstuk geef ik een tentatieve verkenning van wetgevings- en zelfreguleringsinitiatieven in de Verenigde Staten, Japan en een aantal Europese lidstaten. Waar mogelijk illustreer ik deze initiatieven met actuele ontwikkelingen, nieuwe of bijzondere toepassingen van RFID-technologie en discussies tussen voor- en tegenstanders van RFID.

8.2 Zelfregulering of overheidsregulering?

Hoewel het grote publiek naar waarschijnlijkheid pas in een later stadium met grootschalige 'item-level tagging' te maken krijgt (zie hoofdstuk 2), lijken marktpartijen in binnen- en buitenland zich goed te realiseren dat grootschalige invoering van RFID alleen succesvol kan zijn als de consument dit ook accepteert. Er zal daarom vroegtijdig aandacht gegeven moeten worden aan de geuite privacybezwaren. De vraag die in veel landen wordt gesteld is of de overheid hierbij regulerend moet optreden of dat marktpartijen zelf het initiatief dienen te nemen om tot afspraken te komen over de randvoorwaarden voor, en eventuele grenzen aan, de toepassing van RFID. In Nederland is door diverse partijen gepleit om eerst zelfreguleringsinitiatieven een kans te geven.[106] De bepalingen uit de Wbp

[106] Zie onder meer de aanbevelingen van de Werkgroep Privacy & RFID, Schermer, B.W. (2004). RFID: Big Brother in een kleine chip?, in: *JAVI* 2004-4; Koëter, J., & Stuurman, C. (2005). RFID: marktpartijen zijn aan zet; niet de overheid. *Automatiserings Gids*, 17.

zouden hierbij als leidraad kunnen dienen. Het succes van zelfregulering staat of valt met de beschikbaarheid van effectieve handhavingsmechanismen: zonder handhaving kan geen adequaat niveau van bescherming worden geboden. Bits of Freedom (een Nederlandse onafhankelijke stichting die opkomt voor digitale burgerrechten) is echter van mening dat zelfregulering door marktpartijen geen afdoende oplossing is.[107]

De discussie 'overheidsregulering versus zelfregulering' wordt in veel landen gevoerd. De Amerikaanse Federal Trade Commission (FTC) kiest vooralsnog voor het laatste.[108] Zij vindt dat het bedrijfsleven in eerste instantie zelf moet waarborgen dat de privacy van consumenten wordt beschermd bij het gebruik van RFID-technologie. De FTC stelt vast dat veel bezwaren van RFID-toepassingen in feite neerkomen op de beveiliging van de achterliggende databases. Bedrijven die persoonsgegevens verwerken met behulp van RFID moeten daarom volgens de FTC voldoen aan de beveiligingsrichtlijnen die zij hiervoor heeft vastgesteld.

De stellingname van de FTC is met instemming ontvangen door de Amerikaanse RFID-lobby die de wetsvoorstellen in een aantal deelstaten prematuur en te vergaand vindt. De RFID-lobby heeft hierbij steun gekregen van de 'Senate Republican High Tech Task Force', een groep van republikeinse senatoren die heeft verklaard alles in het werk te zullen stellen RFID-technologie te vrijwaren van regulering of van wetgeving 'op zoek naar problemen'.[109]

Consumenten- en burgerrechtenorganisaties zoals het Amerikaanse Privacy Rights Clearinghouse zijn bijzonder kritisch over zelfregulerende initiatieven als de EPC Guidelines (zie hieronder). De negatieve gevolgen van RFID op de privacy en vrijheden van burgers kunnen volgens Clearinghouse alleen worden afgeweerd door richtlijnen voor verantwoord RFID-gebruik wettelijk vast te leggen. Zelfregulering door de industrie zou geen afdoende oplossing zijn vanwege de grote maatschappelijke consequenties van RFID.[110]

8.2.1 RFID Bill of Rights

In oktober 2002 verscheen in de Technology Review (een uitgave van de Massachusetts Institute of Technology) het artikel 'An RFID Bill of Rights' van Simson Garfinkel.[111] In dit artikel beschrijft Garfinkel de mogelijke gevaren voor de

---

107 RFID position paper, Bits of Freedom, 6 december 2004.

108 www.ftc.gov/os/2005/03/050308RFIDrpt.pdf

109 www.republican.senate.gov/httf/index.cfm

110 www.privacyrights.org/ar/RFIDhearing.htm

111 www.technologyreview.com/articles/02/10/garfinkel1002.asp

privacy van burgers als gevolg van het gebruik van RFID. Hij stelt een 'Bill of Rights' voor waarin een aantal consumentenrechten is vastgelegd. Het gaat om het recht:
– te weten of een product een RFID-tag bevat;
– RFID-tags uit te schakelen of te verwijderen wanneer een product gekocht wordt;
– van diensten gebruik te maken zonder RFID-tags, terwijl deze normaliter wel van RFID gebruikmaken;
– kennis te nemen van de in een RFID-tag opgeslagen informatie;
– te weten wanneer, waar en waarom RFID-tags gelezen worden.

De RFID Bill of Rights is opgesteld als een raamwerk voor zelfregulerende initiatieven vanuit het bedrijfsleven en niet zozeer als basis voor nieuwe wetgeving. De Bill of Rights is gedeeltelijk verwerkt in de EPC Guidelines.

8.2.2 EPC Guidelines

EPC Global (de organisatie die de standaard voor de Elektronische Product Code beheert) heeft een aantal richtlijnen opgesteld voor verantwoord gebruik van EPC RFID-tags.[112] De EPC Guidelines dienen als aanvulling op al bestaande nationale en internationale wet- en regelgeving en moeten het vertrouwen van consumenten in het gebruik van RFID en het EPC-netwerk stimuleren. De richtlijnen bevatten vier kernpunten:
– *Consumer Notice*. Consumenten moeten op de hoogte worden gesteld van de aanwezigheid van EPC RFID-tags. Hiertoe dient een vermelding te worden opgenomen op het product of de verpakking.
– *Consumer Choice*. Consumenten moeten geïnformeerd worden over de mogelijkheden om EPC RFID-tags te verwijderen of uit te schakelen wanneer deze gekocht worden.
– *Consumer Education*. Consumenten moet de mogelijkheid worden geboden om snel en eenvoudig duidelijke informatie te krijgen over EPC, de toepassingen ervan en toekomstige ontwikkelingen op het gebied van EPC. Bedrijven die gebruikmaken van ECP RFID-tags in consumentengoederen moeten consumenten bekendmaken met het EPC-logo en de voordelen van RFID.
– *Record Use, Retention and Security.* De EPC RFID-tag bevat zelf geen persoonsgegevens. Het verwerken van persoonsgegevens gegenereerd door het achterliggende EPC-systeem dient in overeenstemming te zijn met alle toe-

[112] www.epcglobalinc.org/public_policy/public_policy.html

passelijke wet- en regelgeving. Bedrijven die gebruikmaken van EPC dienen kenbaar te maken (bijvoorbeeld door publicatie op hun website) wat hun beleid is met betrekking tot de verwerking en bescherming van persoonsgegevens, vooral die persoonsgegevens die gegenereerd en/of verwerkt worden door het EPC-systeem.

Zoals gezegd is de beschikbaarheid van een handhavingsmechanisme bepalend voor de effectiviteit van een zelfreguleringsinitiatief. De EPC Guidelines voorzien hier (nog) niet in. Het naleven van de EPC Guidelines door marktpartijen zou echter niet vrijblijvend hoeven te zijn: EPCglobal heeft immers de macht bedrijven te straffen die zich niet aan de richtlijnen houden door te weigeren EPC's uit te geven of hen de toegang tot het EPC-Netwerk te weigeren.
Garfinkel is sceptisch over de bescherming die de EPC Guidelines bieden aan consument.[113] Consumenten moeten weliswaar op de hoogte worden gesteld van de aanwezigheid van RFID-tags, dit geldt echter niet voor de aanwezigheid van eventuele RFID-readers in een winkel of een andere openbare ruimte. Verder eisen de richtlijnen weliswaar dat consumenten worden geïnformeerd over de verwerking van hun persoonsgegevens, maar nergens is vastgelegd wat de beperkingen zijn. Een bedrijf – zo stelt Garfinkel – kan met de verzamelde gegevens doen en laten wat zij wil, en daarbij nog steeds voldoen aan de EPC Guidelines. Garfinkel lijkt hier over het hoofd te zien dat de richtlijnen wel degelijk eisen dat de gegevensverwerking moet voldoen aan alle toepasselijke wet- en regelgeving zodat zijn kritiek niet helemaal terecht is.

ICC Principles
Ook de International Chamber of Commerce (ICC) heeft onlangs een set richtlijnen geïntroduceerd voor een zorgvuldig gebruik van EPC systemen.[114] Deze richtlijnen gelden in aanvulling op toepasselijke privacyregelgeving en zijn gericht op alle partijen die hier gebruik van (gaan) maken. De richtlijnen bevatten zeven artikelen met onder meer regels over de informatievoorziening aan consumenten, etikettering en keuzemechanismen voor de consument, regels over de openheid die bedrijven moeten betrachten met betrekking tot het gebruik van EPC (bijvoorbeeld via een privacy policy), regels over de gegevensverzameling en doelbinding en regels over het recht op toegang en beveiliging.

---

[113] www.technologyreview.com/articles/04/11/wo_garfinkel110304.asp?p=1

[114] ICC principles for responsible deployment and operation of electronic product codes. Zie www.iccwbo.org/id600/index.html

8.3 Verenigde Staten

In de Verenigde Staten was eind 2004 ongeveer een derde van de burgers bekend met RFID.[115] Meer dan de helft hiervan maakt zich zorgen over hun privacy als het om RFID gaat. De felle anti-RFID-lobby in de Verenigde Staten zou kunnen worden verklaard vanuit het feit dat er minder sterke wetgeving geldt voor de bescherming van persoonsgegevens dan in Europa. Dit verklaart mede het grote aantal wetgevingsinitiatieven.

8.3.1 CASPIAN RFID Right to Know Act (2003)[116]

De Amerikaanse burgerrechtenorganisatie CASPIAN (Consumers Against Supermarket Privacy Invasion and Numbering) protesteert al sinds 1999 tegen technologieën die consumenten bespioneren. De organisatie staat bijzonder kritisch tegenover het gebruik van RFID-tags in consumentenproducten. Via onder meer de websites www.nocards.org en www.spychips.com worden consumenten geïnformeerd over de toepassingsmogelijkheden en privacybedreigingen van RFID-tags. Het blijft niet bij voorlichting alleen. In januari 2005 werd een wereldwijde boycot van de Britse supermarktketen Tesco aangekondigd, met 2.300 winkels een van de grootste retailers in de wereld.[117] Tesco zou zich volgens CASPIAN schuldig maken aan het taggen van individuele producten ('item-level tagging') wat zou leiden tot omvangrijke dataverzameling. Door middel van datamining zou gedetailleerde informatie kunnen worden verkregen over het leef- en bestedingsgedrag van Tesco-consumenten.
Ook op wetgevingsgebied heeft CASPIAN haar bijdrage geleverd. In 2003 heeft zij een modelwet opgesteld die het gebruik van RFID zou moet reguleren. De modelwet zou de US Code of Federal Regulations moeten amenderen en kent de volgende hoofdpunten:

– de verplichting om producten die een RFID-tag bevatten te voorzien van een label waarop is aangegeven dat het product een RFID-tag bevat;
– een bepaling die het aanbrengen van een onduidelijk label dat aangeeft dat een product een RFID-tag bevat, bedreigt met sancties gelijk aan die welke gelden voor het verkeerd of niet labelen van producten;

115 Big Research & Artafact (2004). RFID Consumer Buzz Report.
116 www.spychips.com/press-releases/right-to-know-bill.html
117 Zie onder meer www.boycotttesco.com

– het verbod voor bedrijven om persoonsgegevens te koppelen aan informatie vastgelegd in individuele RFID-tags, anders dan wat noodzakelijk is voor voorraadbeheer;
– een verbod voor bedrijven om persoonsgegevens in samenhang met identificerende informatie uit een RFID-tag te verstrekken aan derden;
– een aanwijzing aan de Federal Trade Commission (FTC) om richtlijnen voor bedrijven op te stellen ter waarborging van de integriteit, vertrouwelijkheid en beveiliging van persoonsgegevens;
– een aanwijzing aan de FTC om te waarborgen dat gegevens verkregen uit RFID-tags geen personen kunnen identificeren;
– een aanwijzing aan de FTC om individuen te beschermen tegen mogelijke (toekomstige) bedreigingen voor de veiligheid van persoonsgegevens en negatieve gevolgen voor het individu die hier het gevolg van kunnen zijn;
– een aanwijzing aan de FTC om burgers en bedrijven voor te lichten over het gebruik van RFID en de mogelijke negatieve gevolgen die dit kan hebben voor de privacy van de burger.

De CASPIAN modelwet heeft als voorbeeld gediend voor specifieke voorstellen voor RFID-wetgeving in een aantal Amerikaanse staten.[118]

8.3.2 RFID Right to Know Act 2004 (California)

In februari 2004 is door senator Bowen een wetsvoorstel ingediend dat het gebruik van RFID-systemen zou moeten reguleren.[119] In tegenstelling tot het wetsvoorstel van CASPIAN richt de aanpassing zich niet op federale wetgeving, maar op aanpassing van de wet in de deelstaat California. Het wetsvoorstel bevat de volgende punten:

Wanneer een RFID-systeem gebruikmaakt van RFID-tags gekoppeld aan consumentenproducten of van een reader die het mogelijk maakt om door het lezen van RFID-tags op consumentenproducten informatie te verzamelen, op te slaan, te gebruiken of te delen die kan worden gebruikt om een persoon te identificeren, is voor een bedrijf niet toegestaan dit systeem te gebruiken tenzij:

---

[118] In 2005 is RFID-wetgeving voorgesteld in California, Maryland, Massachusetts, Missouri, Nevada, New Hampshire, New Mexico, Rhode Island, South Dakota, Tennessee, Texas en Utah. Niet al deze voorstellen hebben overigens hetzelfde voorwerp als de RFID Right to Know Act van CASPIAN. Zie www.ncsl.org/programs/lis/privacy/RFID05.htm

[119] S.B. 1834.

– de reikwijdte van de verzamelde informatie niet verder gaat dan bij wet wordt toegestaan;
– de informatie door een klant aan het bedrijf wordt verstrekt om de afhandeling van een overeenkomst met betrekking tot het kopen of huren van een product met RFID-tag mogelijk te maken;
– de informatie niet verzameld wordt vóór het moment dat de klant daadwerkelijk de overeenkomst tot het kopen of huren van een product met RFID-tag aangaat en na het moment dat de overeenkomst is afgehandeld;
– de informatie alleen betrekking heeft op de klant die daadwerkelijk een product met RFID-tag wil kopen of huren en alleen met betrekking tot dat specifieke product.

Voor een bibliotheek gelden dezelfde voorwaarden, maar dan met betrekking tot de boeken die worden geleend. Een belangrijke omissie in dit wetsvoorstel is de afwezigheid van een definitie van het begrip RFID. Hoewel senator Bowen heeft verklaard dat de wetgeving alleen van toepassing is op die RFID-systemen waarmee persoonsgegevens verwerkt worden, leidt de afwezigheid van een definitie tot veel onzekerheid over de precieze reikwijdte en invulling van de wet.
Het wetsvoorstel heeft een aantal amendementen ondergaan en het is in april 2004 door de State Senate goedgekeurd. Eind juni 2004 is het wetsvoorstel echter verworpen in de State Assembly. Tegenstanders hebben de meerderheid van de Committee Members overtuigd dat de timing van het wetsvoorstel verkeerd was en dat het ongepast zou zijn een wetsvoorstel aan te nemen dat technologie zou reguleren voordat duidelijk was hoe de RFID-tags gebruikt zouden worden in de praktijk.
In februari 2005 is door de democratische senator Simitian een nieuw wetsvoorstel ingediend dat het gebruik van RFID-tags in overheidsdocumenten zou verbieden.[120] Ook het heimelijk uitlezen van overheidsdocumenten zou strafbaar worden. RFID-tags in paspoorten, rijbewijzen en bibliotheekkaarten leiden er volgens Simitian toe dat identiteitsdiefstal eenvoudiger wordt en de privacyrechten van burgers onnodig worden geschaad. Het wetsvoorstel werd aanvankelijk goedgekeurd door de State Senate maar na een hoorzitting van de zogenoemde Assembly's Judiciary Committee werd het voorstel zodanig aangepast dat het verbod slechts voor drie jaar zou gelden. De toekomst van het wetsvoorstel is op dit moment hoogst onzeker nu het voorstel in de zogeheten 'inactive file' is

[120] Voorstel voor de 'Information Protection Act 2005', S.B. 682.

geplaatst. Mocht het wetsvoorstel worden aangenomen dan zal dit zeker niet voor 1 januari 2007 de status van wet krijgen.[121]

8.3.3 RFID Right to Know Act 2004 (Utah)[122]

In Utah is ook een wetsvoorstel ingediend om het gebruik van RFID te reguleren, maar dat voorstel is vooralsnog van de baan. Nadat de wet goedgekeurd was door de Business and Labor Committee en het Huis van Afgevaardigden van Utah, verliep de indieningstermijn bij de Senaat van Utah. Detailhandelaren hadden geklaagd dat het wetsvoorstel het taggen van producten voor voorraad- en trackingdoeleinden onmogelijk zou maken en eisten aanpassing. Mogelijk zal het voorstel opnieuw worden ingediend op een later tijdstip. Het voorstel bevatte de volgende punten:

– de verplichting om producten die een RFID-tag bevatten te voorzien van een label waarop is aangegeven dat het product een RFID-tag bevat, of indien dit niet mogelijk is, een waarschuwing nabij het product (bijvoorbeeld op het schap);
– de verplichting om RFID-tags uit te schakelen bij het verlaten van de winkel, tenzij een consument uitdrukkelijk aangeeft de tag actief te willen houden.

8.3.4 Right to Know Act 2004 (Missouri)[123]

Ook in de staat Missouri is een RFID Right to Know Act ingediend. Het voorstel kent slechts één bepaling: de verplichting om producten die een RFID-tag bevatten te voorzien van een label waarop is aangegeven dat het product een RFID-tag bevat. Ook dit voorstel is vooralsnog gestrand.

8.3.5 Texas

In maart 2005 werd in Texas een wetsvoorstel ingediend dat het papieren kentekenbewijs zou vervangen door een RFID-tag.[124] De RFID-tag (die achter de voorruit van een auto geplakt zou moeten worden) zou het eenvoudiger maken om onverzekerde automobilisten en tolontduikers op te sporen. Het wetsvoorstel liet echter ruimte om de RFID-tag ook voor andere handhavingsdoeleinden in te zetten. Na felle protesten is besloten het wetsvoorstel aan te passen en is de

---

[121] Voor een overzicht van de turbulente ontwikkelingen van wetsvoorstel S.B. 682 en 768 zie: www.blog.librarylaw.com/librarylaw/2005/09/breaking_news_c.html

[122] H.B. 251.

[123] S.B. 128.

[124] H.B. 2893.

RFID-tag geschrapt. Een ander wetsvoorstel over het gebruik van RFID-tags in schoolidentiteitskaarten is voorlopig uitgesteld.[125]

Tot op heden zijn pogingen om op deelstaatniveau RFID-wetgeving te realiseren weinig succesvol gebleken. De roep om zelfregulering en de strijd tegen overheidsregulering door de republikeinse High Tech Task Force en andere RFID-voorstanders hebben hier ongetwijfeld aan bijgedragen. Wetgeving die het gebruik van RFID op federaal niveau moet borgen (zie de modelwet van CASPIAN) lijkt op dit moment zeker geen haalbare kaart. Een aantal auteurs heeft onderzocht of bestaande federale wetgeving eventueel geschikt zou zijn om onrechtmatig gebruik van RFID (althans één aspect daarvan) te sanctioneren.[126] Het zou hierbij gaan om het op afstand heimelijk uitlezen van RFID-tags. Dit wordt vaak beschouwd als een van de belangrijkste privacyrisico's van RFID. De auteurs stellen vast dat de federale Electronic Communication Privacy Act (ECPA) hiervoor zou kunnen worden geamendeerd. De ECPA verbiedt alle vormen van elektronisch afluisteren, het bezitten van apparatuur die dit mogelijk maakt en het verspreiden van informatie die met dergelijke apparatuur is verzameld. Elektronisch afluisteren is weliswaar niet hetzelfde als het uitlezen van een RFID-tag, het heeft volgens de auteurs wel een aantal overeenkomsten. Door RFID onder de reikwijdte van de ECPA te laten vallen zou het strafbaar worden om RFID-tags heimelijk uit te lezen, te kraken of deze te 'klonen'. Hoewel minder vergaand en daarmee misschien minder aansprekend dan de modelwet van CASPIAN zou aanpassing van de ECPA een belangrijke stap zijn in het beschermen van Amerikaanse consumenten tegen onrechtmatig gebruik van RFID.

8.4 Japan

RFID-technologie wordt al breed ingezet in Japan. Naast de meer gebruikelijke toepassingen zijn er plannen om de kleding van Japanse gevangenen en schoolkinderen te voorzien van RFID-tags.[127] Een consortium van Japanse bedrijven in samenwerking met de overheid is een project gestart genaamd HIBIKI dat onder meer als doel heeft om de kosten van RFID-tags terug te brengen tot 5 yen (ongeveer vier eurocent).[128] Een andere groep bedrijven heeft in september 2005 een

125 H.B. 2953.
126 www.RFIDjournal.com/article/articleview/1401/1/128
127 www.ubiks.net/local/blog/jmt/archives3/004343.html
128 www.eetimes.com/story/OEG20031117S0020

non-profitorganisatie opgericht die moet komen tot een standaard voor RFID-identiteitskaarten voor studenten. Mogelijke toepassingen van deze kaarten zijn toegangscontrole, het gebruik van openbare computers, elektronisch geld, vervoersbewijzen en deelname aan digitale colleges.
Het Ministerie van Economische zaken, Handel en Industrie (Keizai Sangyo Sho) en het Ministerie van Algemene Zaken en Communicatie (Somu Sho) hebben in juni 2004 richtlijnen opgesteld voor het gebruik van RFID ('RFID Privacy Protection Guidelines').[129] Hoewel de richtlijnen geen wettelijke basis hebben, schijnt de praktijk uit te wijzen dat marktpartijen deze richtlijnen naleven. De regering ziet daarom vooralsnog geen noodzaak specifieke wetgeving voor te stellen.
De richtlijnen schrijven onder meer voor dat:
– consumenten moeten worden geïnformeerd over de aanwezigheid van RFID-tags;
– consumenten het recht hebben om te kiezen of ze RFID-tags willen gebruiken;
– gebruikers consumenten moeten informeren over het belang van het gebruik van RFID-tags;
– de Japanse privacywetgeving van toepassing is wanneer RFID-tags worden gekoppeld aan databases met persoonsgegevens;
– gebruikers terughoudend moeten zijn met het gebruik van persoonsgegevens die worden verzameld via RFID-systemen;
– gebruikers moeten waarborgen dat de persoonsgegevens accuraat zijn.

De richtlijnen schrijven voor dat consumenten moeten worden voorgelicht hoe zij kunnen voorkomen dat de RFID-tags worden uitgelezen, bijvoorbeeld door een tag te bedekken met aluminiumfolie of de tag fysiek te verwijderen.

8.5 Europa

In januari 2005 heeft de Artikel 29 Werkgroep (het overlegorgaan van de Europese nationale privacytoezichthouders) een consultatiedocument gepubliceerd over de privacyaspecten en mogelijke risico's van toepassingen van RFID.[130] Een belangrijke conclusie van de Werkgroep is dat de Europese privacyrichtlijnen volledig van toepassing zijn op de verwerking van persoonsgegevens die worden

[129] Zie onder meer www.RFIDbuzz.com/news/2004/japanese_RFID_privacy_guideline_released.html
[130] Artikel 29 Werkgroep (2005). Working Document on Data Protection Issues Related to RFID Technology. 10107/05/EN WP 105.

verzameld via RFID-systemen. Volgens de Werkgroep gelden de privacyrichtlijnen niet alleen voor de gebruikers van RFID-technologie (zoals winkelketens). Ook producenten hebben een zelfstandige verplichting hun producten zodanig te ontwerpen dat de gebruikers hun privacyverplichtingen kunnen uitvoeren en dat betrokkenen (zoals consumenten) hun rechten kunnen uitoefenen.
De bevestiging van de Werkgroep dat de Europese privacyrichtlijnen onverkort van toepassing zijn, heeft in ieder geval in Nederland geleid tot de conclusie dat het vooralsnog niet noodzakelijk is om RFID-specifieke aanvullingen te maken op de Wbp. Aanvullende wetgeving zou in dit stadium namelijk wel eens contraproductief kunnen werken. Nadere invulling aan de abstracte formuleringen van de Wbp in de vorm van (sectorspecifieke) gedragsregels zijn echter wel aan te bevelen.
Veel Europese lidstaten hebben vooralsnog vergelijkbare opvattingen over de noodzaak van RFID-specifieke wetgeving. Voorzover bekend zijn er nog geen lidstaten die hebben besloten tot regulering van RFID van overheidswege. Dit wekt geen verbazing nu alle lidstaten beschikken over privacywetgeving die minimaal hetzelfde beschermingsniveau biedt als de Europese privacyrichtlijnen. Het onderwerp RFID en privacy staat wel hoog op de agenda van Europese toezichthouders, marktpartijen en consumenten- en burgerrechtenorganisaties.
Een aantal organisaties (ICC, EICTA, ICRT en JBCE)[131] heeft gezamenlijk kritiek geuit op het consultatiedocument van de Artikel 29 Werkgroep.[132] De Werkgroep zou onvoldoende hebben verwoord dat veel van de huidige RFID-toepassingen buiten de reikwijdte van de privacyrichtlijn vallen. Ook had meer nadruk moeten worden gelegd op realistische, minder vergezochte voorbeelden van RFID-toepassingen. De organisaties betreuren het dat de Werkgroep het begrip persoonsgegeven in relatie tot RFID-technologie erg breed heeft uitgelegd. Hiermee zou het risico kunnen bestaan dat bijvoorbeeld anonieme data onder de reikwijdte van de privacyrichtlijn zou komen te vallen. Naar mijn mening is deze angst enigszins overtrokken. De Werkgroep erkent immers zelf ook dat de privacyrichtlijn alleen van toepassing is op RFID-technologie wanneer er gegevens worden verwerkt die op de een of andere manier kunnen worden herleid tot een individuele persoon. Hiervan is alleen sprake als er persoonsgegevens op de RFID-tag worden gezet of wanneer de gegevens op de RFID-tag worden gekoppeld aan elders opgeslagen persoonsgegevens. Een terecht punt van kritiek is dat niet alleen uitgegaan zou moeten worden van worst case scenario's en dat een realistisch beeld van de technische (on)mogelijkheden van RFID op zijn plaats is.

---

131 International Chamber of Commerce, de European Information Communications and Consumer Electronics Technology Industry Association, de International Communications Round Table en de Japan Business Council in Europe.
132 www.jbce.org/files/RFID_20050331.pdf

8.5.1 Duitsland

In Duitsland kreeg het RFID-debat begin 2004 een sterke impuls door een proef van de Duitse supermarktketen Metro met RFID-technologie.[133] Naar verluidt wisten de klanten van de 'Future Store' niet dat een RFID-tag was verwerkt in hun klantenkaart.[134] De Duitse digitale rechtenorganisatie Foebud organiseerde een demonstratie tegen het gebruik van RFID-chips.[135] Naar aanleiding van de protesten kondigde Metro aan dat zij geen RFID-tags meer in klantenkaarten zou verwerken. Dit betekent niet dat Metro – net als veel andere grote supermarktketens – is gestopt met RFID.[136] De Future Store in Rheinberg experimenteert nog steeds volop met RFID waarbij een (beperkt) aantal consumentenartikelen is voorzien van een RFID-tag.
Foebud trekt ook ten strijde tegen het gebruik van RFID in toegangskaarten voor het WK voetbal 2006 in Duitsland. Dit wordt beschouwd als het grootste internationale project met RFID-toegangskaarten tot op heden. Er zullen zeker 3,2 miljoen RFID-kaarten worden gedrukt. Op de kaarten zelf komt alleen een naam te staan. Andere gegevens (zoals de locatie van de zitplaatsen) worden op de RFID-tag gezet. WK-voetbal organisator FIFA hoopt zo te voorkomen dat er een levendige handel in vervalste toegangskaarten ontstaat. De Duitse privacytoezichthouder (de Bundesbeauftragter für den Datenschutz) en de regering in Darmstadt waar de Duitse voetbalbond is gevestigd hebben hun bezorgdheid en twijfels geuit over het gebruik van RFID in toegangskaarten.
Duitsland kent op dit moment geen specifieke wetgeving die het gebruik van RFID reguleert. De Bundesdatenschutzgesetz is onverkort van toepassing op de verwerking van persoonsgegevens die worden verzameld met behulp van RFID-systemen. De Bondsraad heeft onlangs wel een wetsvoorstel aangenomen waarmee Duitsland naar verwachting het eerste land ter wereld wordt dat een biometrisch paspoort met RFID-tag gaat invoeren. De tag zal in eerste instantie de persoonsgegevens van de houder bevatten (zoals naam en geboortedatum) en een digitale afbeelding van zijn of haar gezicht.[137] Vanaf maart 2007 zal de tag ook een scan van de linker- en rechterwijsvinger bevatten. Naar verluidt is de RFID-tag alleen uit te lezen wanneer het paspoort is geopend en de RFID-reader een speciale toegangscode heeft berekend. Heimelijk uitlezen zou hierdoor onmogelijk moeten zijn. In maart 2005 heeft de Duitse privacytoezichthouder nog tever-

133 www.future-store.org
134 www.spychips.com/metro/overview.html
135 Zie onder meer www.stopRFID.de/en/index.html
136 http://www.foodproductiondaily.com/news/ng.asp?n=62947-metro-group-RFID-epcglobal
137 www.neuer-reisepass.de/index.php

geefs opgeroepen tot een tijdelijke stop op het gebruik van RFID-tags in paspoorten totdat de techniek volledig uitontwikkeld zou zijn en de privacyissues opgelost.

8.5.2 Verenigd Koninkrijk

Het Britse Ministerie van Handel en Industrie heeft verklaard dat zij vooralsnog geen specifieke wet- en regelgeving zal introduceren. Het ministerie geeft de voorkeur aan zelfregulering maar zal de marktontwikkelingen actief in de gaten houden.[138] Het standpunt van het ministerie is mede bepaald door een proef van warenhuis Marks & Spencer met RFID. Het warenhuis heeft veel waardering gekregen voor de wijze waarop zij de proef heeft uitgevoerd en de proef wordt algemeen beschouwd als een goed voorbeeld hoe een bedrijf verantwoord kan omgaan met RFID-technologie.[139] RFID-tags werden bij M&S niet verborgen of ingenaaid in de kleding. Ook konden klanten de tags bij de kassa laten verwijderen zonder dat zij daarbij bepaalde rechten zouden verliezen (zoals het ruilen van de kleding). De RFID-readers werden tenslotte niet gebruikt bij de kassa zodat de gegevens uit de tag niet werden gekoppeld aan klanteninformatie. De resultaten van de proef waren zo goed dat M&S heeft besloten de proef uit te breiden naar andere filialen.[140] Grootschalige invoering zou uiteindelijk kunnen leiden tot het taggen van 350 miljoen kledingstukken per jaar.

8.5.3 Spanje

De 'Comisión de Libertades e Informática (CLI)', een non-gouvernementele organisatie ter bescherming van de privacyrechten, heeft een rapport uitgebracht naar aanleiding van de conclusies van de Artikel 29 Werkgroep over de gevolgen van RFID-technologie voor de verwerking van persoonsgegevens.[141] De CLI concludeert in haar rapport dat dataverzameling met behulp van RFID-tags zonder toestemming van de betrokkene in strijd moet worden geacht met de privacyrichtlijn. De toestemming moet altijd zijn gebaseerd op volledige informatie zodat bedrijven betrokkenen vooraf en adequaat moeten voorlichten, bijvoorbeeld via internet. Dit standpunt lijkt moeilijk verenigbaar met de privacyrichtlijn die vele mogelijkheden biedt om persoonsgegevens te verwerken zonder de toe-

138 www.liberty-human-rights.org.uk/ privacy/RFID-parli-briefing.pdf
139 www.spychips.com/marks_and_spencer.htm
140 www.RFIDjournal.com/article/articleview/791/1/1
141 www.asociacioncli.org

stemming van betrokkene. De CLI roept de Europese Unie op om specifieke wetgeving te ontwerpen met betrekking tot RFID-technologie. Totdat deze van kracht is zou iedere lidstaat specifieke regels terzake moeten opstellen. Deze oproep is niet verstandig. Mocht specifieke wetgeving al noodzakelijk blijken, dan zal dit toch minimaal in Europees verband moeten gebeuren

8.5.4 Italië

De Italiaanse privacytoezichthouder (Garante per la protezione zdei dato personali) heeft in maart 2005 een rapport uitgebracht waarin zij verklaart dat RFID-technologie kan leiden tot inbreuk op privacyrechten.[142] De toezichthouder ziet vooral gevaar in de mogelijkheid om tags en readers te verbergen. Strikte naleving van de Italiaanse Wet bescherming persoonsgegevens is daarom van groot belang. De toezichthouder maakt een eerste aanzet voor de nadere invulling van de abstracte wettelijke formuleringen voor toepassing in RFID-systemen.

8.6 Conclusie

In veel landen is de roep om regulering van RFID-technologie de laatste jaren sterker geworden. Dit valt goed te verklaren nu de invoering van item-level tagging (de meest verstrekkende toepassing van RFID) langzamerhand dichterbij komt. Het gebruik van RFID-tags in de toegangskaarten voor het WK-voetbal in 2006 is hier een goed voorbeeld van. De vraag of de overheid hierbij regulerend moet optreden of dat marktpartijen zelf tot regulering moeten overgaan wordt wereldwijd verschillend beantwoord. In de Verenigde Staten en Japan krijgt zelfregulering vooralsnog de voorkeur boven overheidsregulering. De talloze Amerikaanse wetgevingsinitiatieven hebben nog tot weinig concreet resultaat geleid. Europese lidstaten hebben weinig redenen tot overhaaste wetgevingsvoorstellen. De Europese privacyrichtlijnen bieden immers een goede (basis)bescherming. Wel is een aantal marktpartijen alvast overgegaan tot het vaststellen van specifieke gedragsregels ter nadere invulling van de abstracte formuleringen uit de privacyrichtlijnen. De praktijk zal uitwijzen of deze bescherming adequaat is of dat de Europese wetgever alsnog tot specifieke aanvullingen op de privacyrichtlijnen zal overgaan.

[142] 'Etichette intelligenti (Rfid)': il Garante individua le garanzie per il loro uso – 9 marzo 2005.

Afkortingen

3DES	Triple Digital Encryption Standard
AM/FM	Amplitude Modulated/Frequency Modulated
AES	Adavanced Encryption Standards
AIDC	Automatische Identificatie and Data Capture
BOF	Bits of Freedom
BW	Burgerlijk Wetboek
CASPIAN	Consumers Against Supermarket Privacy Invasion and Numbering
CBP	College bescherming persoonsgegevens
CDRH	Center for Devices and Radiological Health
CEN	European Committee for Standardisation
CLI	Comisión de Libertades e Informática
CRM	Customer Relation Management
DNS	Domain Name System
DoS	Denial of Service
EAS	Electronic Article Surveillance
ECPA	Electronic Communication Privacy Act
EMD	elektronisch medicatiedossier
EMI	Electromagnetic Interference, elektronischmagnetische interferentie
EMP	Electromagnetic Pulse
EPC	Electronic Product Code
EPC-DS	Electronic Product Code Discovery Services
EPC-IS	Electronic Product Code Information Services
EPD	Elektronisch Patiënten Dossier
ERP	Enterprise Resource Planning
EU	Europese Unie
EVRM	Europees Verdrag voor de Rechten van de Mens
FDA	the Food and Drug Administration
FTC	Federal Trade Commission
GHz	Giga Hertz
GPS	Global Positioning System
GSM	Global System for Mobile Communications
HF	High Frequency
ICC	International Chamber of Commerce

ICT	Informatie- en communicatietechnologie
ID	Identificatie, identification
IPv6	Internet Protocol versie 6
ISM	Industrial Scientific Medical (frequentieband)
ISO	International Organisation for Standardisation
LF	Low Frequency
LJN	landelijk jurisprudentie nummer
MHz	Mega Hertz
NAW	naam, adres, woonplaats
ONS	Object Name Service
OV	openbaar vervoer
PC	Personal Computer
PDA	Personal Digital Assistent
PKI	Public Key Infrastructure
PML	Physical Markup Language
RFID	Radio Frequency Identification
SCM	Supply Chain Management
SHF	Super High Frequency
Sr	Wetboek van Strafrecht
Tw	Telecommunicatiewet
UCC	Uniform Code Council
UHF	Ultra High Frequency
UZI	unieke zorgverlener identificatie
UZIVO	unieke zorgverzekeraar identificatie
Vb	Vrijstellingsbesluit
VIP	Very Important Person
VK	Verenigd Koninkrijk
VS	Verenigde Staten
Wbp	Wet bescherming persoonsgegevens
WDH	waarneemdossier huisartsen
WiFi	Wireless Fidelity
WOR	Wet op de ondernemingsraden
XML	Extensible Markup Language

Over de auteurs

Peter Blok
Peter Blok is als advocaat werkzaam bij de sectie Intellectuele Eigendom & Informatietechnologie van Houthoff Buruma te Amsterdam. Hij is gespecialiseerd in vraagstukken op het gebied van de Wet bescherming persoonsgegevens en overige privacyregelgeving. Verder adviseert en procedeert hij op diverse terreinen van het IT-recht. Hij is gepromoveerd op het proefschrift 'Het recht op privacy. Een onderzoek naar de betekenis van het begrip "privacy" in het Nederlandse en Amerikaanse recht'. Een deel van zijn promotieonderzoek heeft hij als visiting researcher verricht aan de rechtenfaculteit van Georgetown University in Washington DC. Hij studeerde rechten en wijsbegeerte aan de Universiteit van Leiden.

Roel Croes
Roel Croes is adviseur bij Croes Consultants. Met een focus op ICT, juridische zaken en innovatie adviseert hij bedrijven in bedrijfsoptimalisatie. Hij werkte onder meer voor diverse triple play organisaties. Croes studeerde Notarieel en Nederlands recht in Nijmegen. Hij is een gepassioneerd voorstander van innoverend technologisch onderzoek op de terreinen van ICT en duurzaamheid. Daarnaast is hij lid van diverse begeleidingscommissies voor wetenschappelijk technologisch onderzoek.

Jeroen Koëter
Jeroen Koëter studeerde in 1999 af aan de Universiteit Leiden en is thans advocaat bij de sectie Intellectual Property/Information, Communication & Technology van De Brauw Blackstone Westbroek in Amsterdam. Daarvoor werkte hij bij Van Doorne en rechtsvoorgangers. Zijn praktijk omvat het adviseren en procederen op het terrein van het IT-recht, waaronder outsourcing, het opstellen en onderhandelen van IT-contracten, mislukte automatiseringsprojecten, e-commerce en privacy. Ook publiceert en doceert hij af en toe op deze terreinen.

Bart Schermer
Bart Schermer is als juridisch adviseur bij ECP.NL, platform voor eNederland, werkzaam op de gebieden privacy, computercriminaliteit en zelfregulering. Hij is secretaris van de Juridische Expert Groep en de Werkgroep RFID & Privacy van

ECP.NL en vice chair van de UN/CEFACT Legal Group. Naast zijn werk voor ECP.NL draagt Bart sinds januari 2005 de verantwoordelijkheid voor het RFID Platform Nederland, een stichting die de toepassing van RFID in Nederland stimuleert. Voorts is hij als onderzoeker verbonden aan eLaw@Leiden, het Centrum voor Recht in de Informatiemaatschappij van de Universiteit Leiden, alwaar hij promotieonderzoek verricht naar de verhouding tussen sociale controle en individuele vrijheid bij het gebruik van softwareagenten.

Jeroen Terstegge
Jeroen Terstegge is Corporate Privacy Officer van Koninklijke Philips Electronics. In die rol adviseert hij Philips Semiconductors, wereldwijd marktleider in RFID-technologie, over de privacyrisico's van RFID. Tevens is hij Issue Manager RFID & Privacy voor EICTA (de vereniging voor de Europese ICT-industrie) in Brussel, en is hij lid van de commissie voor zorgvuldig gebruik van RFID-technologie van de Internationale Kamer van Koophandel (ICC) in Parijs, alsmede van de Public Policy Steering Committee van EPCGlobal Inc., de standaardisatieorganisatie voor de Electronic Product Code. Hij is een veelgevraagd spreker voor het onderwerp RFID en Privacy en heeft lezingen gehouden bij de OESO, de Europese Commissie, en de Internationale Conferentie van Privacyautoriteiten.

Jessica Verwer
Jessica Verwer is student rechten aan de Universiteit Leiden en stagiair bij ECP.NL. Haar afstudeerscriptie heeft als onderwerp de privacy van werknemers bij het gebruik van RFID.

Gerrit-Jan Zwenne
Gerrit-Jan Zwenne is advocaat bij Bird & Bird in Den Haag. Hij adviseert telecom- en andere bedrijven in allerlei juridische procedures over uiteenlopende vragen op het gebied van telecom- en privacyrecht. Verder is hij verbonden aan eLaw@Leiden, het Centrum voor Recht in de Informatiemaatschappij van de Universiteit Leiden en het E.M. Meijers Instituut van dezelfde universiteit. In die context geeft hij geregeld colleges en cursussen over de dingen waar hij verstand van heeft en publiceert hij af en toe een artikel of boek over de onderwerpen waar zijn belangstelling naar uitgaat.