Radio Frequency Identification

Fictie wordt werkelijkheid en onze privacy staat weer onder druk

Griet Verhenneman

Onder wetenschappelijke leiding van Prof. Dr. Jos Dumortier

1. INLEIDING

Radio Frequency Identification of RFID is een nieuwe technologie die het gegevensbeheer en de gegevensverwerking danig zal vergemakkelijken. De vraag is nu of een grootschalig gebruik van deze geautomatiseerde technologie geen inbreuken op de privacy met zich zal meebrengen. Aangezien de technologie zelf nog erg ongekend is start ik met een kort onderzoek naar de verschillende types en toepassingen van RFID. Daarna behandel ik het huidig westerse privacybegrip gevolgd door de wetgeving die hier rond bestaat en bekijk ik of de RFID technologie onder deze wetgevingen valt. De al dan niet rechtmatige verwerking van persoonsgegevens wordt daarbij de belangrijkste vraag. Verder behandel ik de vraag of de bestaande wetgeving voldoende bescherming biedt. Tot slot bekijk ik hoe de problemen rond RFID en privacy in Nederland en in Amerika beoordeeld worden en doe ik enkele suggesties tot wetswijziging.

2. RFID-TAGS: HET NIEUWE CREDO VAN GEGEVENSBEHEER

RFID of Radio Frequency Identification is een technologie gebaseerd op radiogolven die gegevensbeheer een stuk eenvoudiger, sneller én efficiënter maakt. Ze bestaat al sinds de tweede wereldoorlog, maar wordt nu pas goedkoop genoeg om op grote schaal gebruikt te worden.

2.1. WAT IS RFID?

De RFID-technologie is gebaseerd op kleine chips die een radiosignaal kunnen ontvangen en terugzenden. Het grote voordeel van RFID is dat dit signaal automatisch kan geregistreerd worden. Er geen komt scanning of andere

handeling meer aan te pas. Het uitgezonden radiosignaal bevat een identificatiecode. Door die unieke code op te zoeken in een centrale database krijgt het uitgezonden signaal een betekenis en creëert men als het ware een "*Internet van de dingen*"[1]. Een voorbeeld van zo een centrale database is de Electronic Product Code database (EPC). Het is deze database die veelbelovend is voor de retail.

2.2. GESCHIEDENIS EN ONTWIKKELING VAN DE RFID TECHNOLOGIE

2.2.1. Ontstaan van de RFID-technologie

Alles begon met de ontwikkeling van een systeem door het Britse leger in 1939 om oorlogsvliegtuigen in de lucht te kunnen identificeren. Elk vliegtuig zendt een uniek radiosignaal uit. Indien het signaal teruggezonden werd wist men dat het een eigen vliegtuig was, werd het niet teruggezonden was het vijandig.

De recente enorme belangstelling voor RFID is het gevolg van ten eerste een verhoogde vraag naar veiligheid in de samenleving, maar vooral nog van de hang naar economisch efficiëntere technologieën. Door de voortschrijdende stand van de techniek wordt de RFID-technologie steeds goedkoper én worden de onderdelen ervan, met name de chips, ontvangers en antennes, steeds kleiner en dus gemakkelijker in te werken in producten[2].

2.2.2. De verschillende types van RFID

Er moet een onderscheid gemaakt worden tussen de passieve en de actieve RFID-tags of tussen de tags zonder en met eigen energiebron[3].

2.2.2.1. De passieve tags

De passieve tags hebben geen eigen, interne energiebron. Het binnenkomende radiosignaal zal juist genoeg energie opwekken in de tag om een nieuw signaal uit te zenden. Daarna "slaapt" de tag opnieuw.

---

[1] Communication from the commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, *Radio Frequency Identification (RFID) in Europe: steps towards a policy framework*, 2007, http://ec.europa.eu/information_society/policy/rfid/doc/rfid_en.pdf, laatst geconsulteerd op 7 mei 2007, 3; Legal IST Project, *Report on additional legal issues*, 2006, http://www.ve-forum.org/projects/P1507/D15%20Report%20on%20Additional%20Legal%20Issues%20-%20final%20version.pdf, laatst geconsuleerd op 5 mei 2007, 11.

[2] W. SCHREURS, "Privacy en RFID-technologie", *P&I*, 2005, nr. 5, 197-198; B. SCHERMER, "Big Brother in een kleine chip?", 2004, *JAVI (Ned.)*, nr. 5, 161; Wikipedia, the free online encyclopaedia, http://en.wikipedia.org/wiki/RFID en http://nl.wikipedia.org/wiki/RFID.

[3] Legal IST Project, *o.c.*, 38; Wikipedia, the free online encyclopedia, *o.c.*; Opmerking: de auteurs voegen hieraan ook nog de semi-actieve tags als een derde categorie toe, waarbij het verschil tussen de actieve en de semi-actieve tag ligt in de opgeslagen gegevens, maar dat onderscheid laat ik verder buiten beschouwing daar ik denk dat het niets toevoegt aan de discussie.

Het voordeel van de passieve tags is dat zij, juist doordat ze geen interne energiebron behoeven, zeer klein kunnen zijn. Sommigen zijn niet groter dan een speldenkop en dus heel moeilijk met het blote oog waarneembaar, anderen worden verwerkt in stickers. Daarenboven hebben zij een zeer eenvoudig ontwerp waardoor ze goedkoop en in grote hoeveelheden gefabriceerd kunnen worden.

2.2.2.2. De actieve tags

De actieve tags hebben wel een eigen, interne energiebron om een signaal uit te zenden. In principe kan er tussen een actieve tag en een reader dan ook een gesprek ontstaan.

Het voordeel van de actieve tags is dat zij een sterker, verder dragend signaal kunnen uitzenden. Daardoor kunnen ze ook gebruikt worden in massa's waarin radiosignalen zich moeilijker verplaatsen zoals door water of metalen containers en waardoor ze bijvoorbeeld ook ingepland kunnen worden in vee.

2.3. TOEPASSINGEN VAN RFID

2.3.1. De nieuwste hype in retail-land

Het is overduidelijk dat de voordelen van de RFID-technologie in de retail enorm zijn. Zowel op het vlak van efficiëntie als op het vlak van marketing.

Wat betreft de efficiëntie is het een groot voordeel dat de tags automatisch gelezen worden. Daarenboven werken ze van op een afstand. Bij RFID speelt m.a.w. het *line-of-sight* probleem geen rol meer: i.p.v. een kassierster achter een scanner te zetten, wandelen we met RFID gewoon door een poortje. Verder kunnen er ook zeer gedetailleerde gegevens verzameld worden over gemiddelde opslagtijden en vervoerstijden en over hoe vaak producten weggegooid moeten worden omdat de versheidsdatum overschreden is[4].

Wat betreft de marketing is de enorme hoeveelheid informatie die op de wel zeer kleine chips kan worden opgeslagen compleet nieuw. Door het gebruik van RFID smart labels krijgt elk product zijn eigen, unieke identificatiecode. Het ene blikje cola is dan het andere niet meer. Daarnaast kan men consumenten volgen in al hun doen en laten, niet alleen op het moment dat men aankopen doet, maar ook over een langere periode. Zo kan men a.h.w. een profiel opstellen van zijn cliënteel als geheel, maar ook van elke individuele klant apart, wanneer de verzamelde gegevens gekoppeld worden aan een identificerend product zoals bijvoorbeeld een klanten- of kredietkaart. Het is hiertegen dat consumentenorganisaties en privacygroeperingen sterk reageren[5].

De voornaamste bezwaren die gemaakt worden zijn ten eerste dat de consument vaak niet weet dat hij een RFID-tag bij zich draagt of niet weet

[4] B. SCHERMER, "Big Brother in een kleine chip?", *JAVI* (Ned.), 2004, 161-162.

[5] Rathenau Instituut, *Naar een internet van kleine dingen, politiek-bestuurlijke kwesties bij de invoering van RFID*, 2006, http://www.erjure.nl, laatst geconsulteerd op 20 februari 2007.

wanneer de chip gelezen wordt, ten tweede dat een profiel kan opgesteld worden van elke individuele klant en ten slotte dat hetzelfde doel vaak even goed bereikt kan worden met het verzamelen van anonieme gegevens[6].

2.3.2. Andere toepassingen van RFID

De mogelijke toepassingen van RFID zijn werkelijk onoverzienbaar. Het lijkt wel alsof de technologie op alles en overal zou toegepast kunnen worden. Enkele voorbeelden:

- in Duitse paspoorten werd reeds een RFID-chip geïntegreerd om iris-informatie, vingerafdrukken en het reisverleden van de persoon op te slagen[7]
- in ziekenhuizen wordt RFID gebruikt in bandjes van of zelfs implantaten bij patiënten ter identificatie en/of om hun medische informatie in op te nemen. Ook op chirurgische instrumenten wordt een chip aangebracht om het risico dat een instrument blijft zitten na een operatie verminderen[8]
- in auto's wordt de sleutel vervangen door een RFID-chip, maar kan bijvoorbeeld ook een RFID-tag ingebouwd worden in de banden die laat weten wanneer ze aan vervanging toe zijn[9]
- in de toegangskaarten van de Wereldbeker voetbal in Duitsland werd een chip ingebouwd zodat men de supportersstroom kon leiden en gevechten kon vermijden, ook in de gebruikte ballen werd een chip ingebouwd zodat men ze gemakkelijk kon terugvinden[10]
- in de Baja Beach Clubs over de hele wereld kan je een RFID-chip laten inplanten waarmee je aan de bar drankjes kan bestellen en toegang krijgt tot de VIP ruimtes[11]
- Een wasmachine zou een seintje kunnen geven wanneer er een rode sok tussen de witte was zit[12]

Het wordt dus stilaan duidelijk dat RFID over enkele jaren niet meer weg te denken zal zijn uit onze maatschappij. Het wordt echter ook duidelijk dat voornamelijk door de enorme massa aan gegevens die verzameld kan en zal worden, de risico's op privacyschendingen niet te onderschatten zijn. Bijgevolg is het de hoogste tijd om na te gaan hoe de privacy vandaag

---

[6] X, *The RFID Privacy Threat*, Consumentenorganisatie o.l.v. Katherine Albrecht, http://www.spychips.com/alec-big-brother-barcode-article.html, laatste geconsulteerd op 22 februari 2007; X, *Working document on data protection issues related to RFID technology*, 2005, website Europese regelgeving, http://www.europa.eu.int/comm/internal-_market/privacy/workinggroup/wp/2005/wpdocs05_en.htm., laatst geconsulteerd op 24 februari 2007, 5.

[7] De Europese Raad nam in 2004 reeds verordening een aan die de opname van iris-informatie en vingerafdrukken in paspoorten toelaat, zie Verord Raad EG nr. 2252/2004, 13 december 2004, *PB L.*, 29 december 2004, 1-6.

[8] X, "RFID-cip bij patiënten in Flevoland", *P&I*, 2005, nr. 3, 134-135.

[9] Wikipedia, the free online encyclopaedia, *o.c.*

[10] W. SCHREURS, "Privacy en RFID-technologie", *P&I*, 2005, nr. 5, 198.

[11] S. NAS, "Iedereen een chippie in zijn arm? RFID-labels en de wolk van gegevens", *P&I*, 2005, nr. 3, 105.

[12] Wikipedia, the free online encyclopaedia, *o.c.*

beschermd wordt en of de huidige privacybeschermingswetgeving ook voor de toekomst kan volstaan.

3. RFID-TAGS EN PRIVACY: LEVEN WE STRAKS ALS IN EEN ACTIETHRILLER?

Ik zie mezelf nog de eerste keer kijken naar *Enemy of the State*, een actiefilm uit 1998 over de uitbreiding van de wetgeving op nieuwe toezichtsmethodes van politie en justitie en de privacyinbreuken die deze met zich meebrengen. D.m.v. hoogstaande satelliettechnologie en zendertjes van alle soorten, verstopt in kleding, horloges en zelfs rookdetectors ontstaat er een spel van achtervolging en spionage. In 1998 leek dit nog pure fictie, nu ik hieraan schrijf stel ik me de vraag of dit straks dagdagelijkse realiteit wordt. Technologisch gezien is het in ieder geval mogelijk. Het is dan ook van belang nu al te kijken naar eventuele gevolgen van deze technologieën op de privacy.
Ik behandel achtereenvolgens het begrip privacy, de voorziene wettelijke bescherming en de vraag in hoeverre de RFID-technologie de privacy en de verwerking van persoonsgegevens raakt. Het is daarbij niet vanzelfsprekend dat producenten, toepassers en gebruikers dezelfde mening hebben over afdoende waarborgen.

3.1. HET WESTERS PRIVACYBEGRIP

"*De behoefte aan privacy is zo oud als de wereld*" schrijft Dr. J. Holvast, toch duikt het recht op privacy pas in de 20ste eeuw op in internationale verdragen en nationale grondwetten. Dat heeft niet enkel met het recht te maken, maar ook met het feit dat het privacybegrip plaats- en tijdsgebonden is. Niet overal staat het individu met zijn vrijheid, privacy en eigendom op een piëdestal. Zo maakt bijvoorbeeld het Afrikaans Handvest voor de Rechten van de Mens helemaal geen vermelding van een recht op privacy, terwijl dat in de Europese versie niet meer weg te denken is. Privacy is dus een begrip dat maar een betekenis krijgt wanneer het geplaatst wordt in een maatschappelijke, culturele, historische en staatkundige context[13].

In de jaren '70 bestond de neiging om het recht op privacy te reduceren tot de informationele privacy of zelfs computerprivacy. Nu blijkt echter dat de computer slechts een voorbode is geweest van een veelheid aan toepassingen van wat "de informatietechnologie" wordt genoemd. Cameratoezicht, biometrie, statistische technieken, het internet, de GPS, maar ook de RFID en de Ambient Technologies maken het collecteren van een berg gegevens over personen mogelijk.

Het recht op privacy wordt zo een bescherming tegen derden die invloed op

[13] J. HOLVAST, "Wet bescherming persoonsgegevens: privacywet of een wet die gegevens beschermt?", *P&I*, 2005, nr. 6, 242-245.

ons zouden kunnen krijgen door kennis van onze persoonsgegevens. Het is daarbij verontrustend dat we steeds minder controle hebben over niet alleen het verzamelen en opslaan van onze gegevens, maar ook over het gebruik ervan. De wijze waarop het bedrijfsleven persoonsgegevens verwerkt wordt steeds ondoorzichtiger, de koppeling van gegevens steeds gemakkelijker. Maar ook de overheid maakt gretig gebruik van de verzameling aan persoongegevens. Criminaliteit en terrorisme lijken een vrijgeleide te vormen voor privacyinbreuken[14].

3.2. WETTELIJKE BESCHERMING VAN HET PRIVACYRECHT

Aan het recht op privacy wordt in onze maatschappij dus zeer veel belang gehecht. Dat wordt ook gereflecteerd in de plaats die het krijgt in de wetgeving. In alle Westerse landen wordt het recht op een privé-leven aanvaard als een grondrecht. Op Europees niveau wordt het erkend als fundamenteel recht in het EVRM en in het ontwerp van de Europese Grondwet en er werden richtlijnen uitgevaardigd i.v.m. de bescherming van persoonsgegevens.

Toch is het recht op privacy geen absoluut recht. Het gangbare huidige Westerse privacybegrip is dan wel sterk verbonden met het idee dat de maatschappij individuele vrijheid en verscheidenheid moet respecteren, maar ook het algemeen belang van een samenleving daarbij niet mag verwaarloosd worden. [15].

3.2.1. Privacy als grondrecht en mensenrecht

Het recht op privacy wordt zowel in de Belgische Grondwet[16], het UVRM[17] als in het EVRM[18] op een techniek onafhankelijke manier geformuleerd. In alle drie de teksten wordt echter ook benadrukt dat het recht op privacy geen absoluut recht is[19]. Het EVRM stelt daarbij zelfs een aantal expliciete toetsingsgronden voorop. Ten eerste vereist artikel 8 EVRM een legaliteitstoets: de wet moet de inbreuk voorzien hebben. Ten tweede vereist het een noodzakelijkheidstoets: de inbreuk moet noodzakelijk zijn in een democratische samenleving. Ten slotte moet elke inbreuk de legitimatietoets doorstaan: ze moet een legitiem doel nastreven[20].

Ook in de toekomst lijkt het recht op privacy een cruciale rol te zullen blijven spelen. In het Ontwerp tot Europese Grondwet werd de bescherming van de

[14] E. DOMMERING, N. VAN EIJK, J. NIJHOF en M. VERBERNE, *Handboek Telecommunicatierecht*, 's-Gravenhage, SDU Uitgevers, 1999, 601-602.
[15] P. HUSTINX, "Data Protection in the European Union", *P&I*, 2005, nr. 2, 62.
[16] Art 22 Gec. GW.
[17] Art 12 UVRM.
[18] Art 8 EVRM.
[19] P. DE HERT, *Privacy en persoonsgegevens*, Brussel, Politeia, 2004, 47-51; ECP.NL, *Privacyrechtelijke aspecten van RFID*, 2005, http://www.ecp.nl/downloads, 16-18.
[20] P. DE HERT, *o.c.*, 79-93; ECP.NL, *o.c.*, 49-50.

fundamentele rechten immers nog sterker benadrukt dan nu reeds het geval is in onze grondwet en de mensenrechtenverdragen. Wat opmerkelijk is, is dat de eerbiediging van het privé- en familieleven en de bescherming van persoonsgegevens als afzonderlijke rechten worden opgenomen[21]. Doordat de bescherming van persoonsgegevens daarenboven ook nog eens vermeld wordt in het deel I van de grondwet[22], dat handelt over het democratisch leven in de Unie, wordt de bescherming van persoonsgegevens daarenboven een noodzakelijk element van *good governance*[23].

3.2.2. Richtlijn 95/46/EG betreffende de bescherming van natuurlijke personen i.v.m. de verwerking van persoonsgegevens en de omzettingswet Wet van 11 december 1998

De eerste stap naar de bescherming van persoonsgegevens werd gezet in 1981 met het sluiten van het Verdrag van Straatsburg inzake gegevensbescherming binnen de Raad van Europa. Dit akkoord werd inmiddels omgezet in de verschillende nationale wetgevingen. In België resulteerde dat in de Wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer t.o.v. de verwerking van persoonsgegevens[24].

Er bleken echter grote verschillen te bestaan in de omzettingswetgevingen tussen de verschillende lidstaten en dat vormde een belemmering voor het vrij verkeer binnen de EU. Die belemmeringen vormden een eerste reden voor de Europese Commissie om tussen te komen. In 1995 vaardigde ze de Data Protection richtlijn uit[25]. De richtlijn gebruikt het akkoord uit 1981 als basis, maar specificeerde het en voegde er nieuwe elementen aan toe. Deze richtlijn moest binnen de drie jaar worden omgezet in nationaal recht en dat heeft in België geleid tot de Omzettingswet van 11 december 1998 die de Wet van 8 december 1992 heeft vervangen[26].

Een tweede reden voor het creëren van een afzonderlijke bescherming voor de verwerking van persoonsgegevens was de vaststelling dat een onverkorte toepassing van de traditionele leer rond het recht op eerbiediging van het privéleven, tot een uitholling leidde van de bescherming tegen verwerking van persoonsgegevens. Door het recht op eerbiediging van het privéleven in de context van persoonsgegevens te interpreteren als een vrijheid i.p.v. een recht, krijgt ieder individu de vrijheid om bijzondere relaties te onderhouden, gevrijwaard van elke externe inmenging. Zo kunnen ook verwerkingen van

[21] art II-67 en II-68 Ontwerp tot Europese Grondwet.
[22] art I-51 Ontwerp tot Europese Grondwet.
[23] P. HUSTINX, "Data Protection in the European Union", *P&I*, 2005, nr. 2, 62-65.
[24] *B.S.*, 18 maart 1993.
[25] Richtl. Eur. Parl. en Raad E.G. nr. 95/46, 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens, *PB L.*23 november 1995, 31–50.
[26] *B.S.*, 3 februari 1999; P. HUSTINX, *o.c.*, 62-63; J. DUMORTIER, "Privacybescherming bij de verwerking van persoonsgegevens", in *Mediarecht, Telecommunicatie en telematica*, Mechelen, Kluwer, 1999, Afl. 12, 59-62.

persoonsgegevens die geen inbreuk op het privé-leven vormen, maar wel op andere rechten, aangepakt worden[27].

Ook de Richtlijn van 1995 en de Wet van 11 december 1998 hebben een techniekonafhankelijke formulering en kunnen dus in principe zonder problemen toegepast worden op de RFID. Artikel 3 van de wet bepaalt dat de wet van toepassing is op *elke geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens die opgenomen zijn in een bestand of bestemd zijn om daarin opgenomen te worden*, maar niet wanneer de gegevens bestemd zijn voor persoonlijk gebruik of gebruik voor openbare statistiek en journalistieke, literaire of artistieke doeleinden[28].

3.2.3. De richtlijn elektronische handel 2002/58/EG

In 2000 werd een nieuwe richtlijn opgesteld om het hoofd te bieden aan de razendsnelle opkomst van elektronische transacties[29]. Ook in deze richtlijn is het hoofddoel het vrijwaren van het vrij verkeer en dan meerbepaald op gebied van de diensten van de informatiemaatschappij. Dat neemt echter niet weg dat ook deze richtlijn bescherming biedt aan de gebruikers van openbare elektronische communicatienetwerken en –diensten[30]. Inhoudelijk gebruikt de richtlijn meestal gelijkaardige begrippen als de Data Protection richtlijn, maar de extra waarde van deze richtlijn ligt in haar aanzet tot een recht op anonimiteit.

Over de al dan niet toepasselijkheid van de richtlijn op RFID bestaat echter grote twijfel. Langs de ene kant wordt benadrukt dat de richtlijn ontworpen is om technologieonafhankelijk te zijn en dat ze van toepassing is op elke communicatie waarbij gegevens worden uitgewisseld. Langs de andere kant wordt echter geargumenteerd dat RFID om wettechnische redenen niet onder de communicatiedefinitie van de richtlijn kan worden gebracht. De definitie van een elektronisch communicatienetwerk komt voort uit de kaderrichtlijn 2002/21/EG[31]. Die richtlijn stelt dat zij niet van toepassing is op apparatuur die onder de RTE-richtlijn[32] valt. Onder de RTE-richtlijn valt alle radioapparatuur.

---

[27] D. DE BOT, *Privacybescherming bij e-government in België* in *CPR Collectie Publiekrecht*, Brugge, Vanden Broele, 2005, 14-15.

[28] J. DUMORTIER, "Privacybescherming bij de verwerking van persoonsgegevens", in *Mediarecht, Telecommunicatie en telematica*, Mechelen, Kluwer, 1999, Afl. 12, 59-62; P. DE HERT, *Privacy en persoonsgegevens*, Brussel, Politeia, 2005, Afl. 16, titel II, 9-10; C. CUIJPERS, *Privacy en persoonsgegevens*, Brussel, Politeia, 2006, Afl. 20, Titel III, 5-8.

[29] Richtl. Eur. Parl. en Raad E.G. nr. 2002/58, 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie, *P.B. L.* 31 juli 2002, 37-47.

[30] P. CAREY, *E-privacy and online data protection*, Londen, Butterworths LexisNexis, 2002, 25-28; D. DE BOT en S. RENETTE, "Employee, where are thou?", *P&I*, 2006, afl. 5, 210-213.

[31] Richtl. Eur. Parl. en Raad E.G., nr. 2002/21, een gemeenschappelijk regelgevingskader voor elektronische-communicatienetwerken en -diensten, *PB L.* 24 april 2002, 33–50.

[32] Richtl. Eur. Parl. en Raad E.G. nr. 1999/5 betreffende radioapparatuur en telecommunicatie-eindapparatuur en de wederzijdse erkenning van hun conformiteit, *PB L.* 7 maart 1999, 10-28; B. SCHERMER, "Big Brother in een kleine chip?", 2004, *JAVI (Ned.)*, nr. 5, 163-164; A. EKKER,

Radioapparatuur omvat elk apparaat dat radiogolven kan uitzenden of ontvangen. Ook de RFID technologie werkt essentieel door het uitzenden en ontvangen van radiogolven[33].

De Europese Commissie heeft geoordeeld dat de richtlijn elektronische handel in een beperkt aantal gevallen van toepassing kan zijn op de RFID-technologie[34]. Artikel 9 van de richtlijn vereist immers dat de verwerking van persoonsgegevens gebeurt binnen een publiek communicatienetwerk en dat netwerk bestaat in beginsel niet bij de toepassing van RFID. Bijgevolg is deze richtlijn enkel van toepassing wanneer RFID gekoppeld wordt aan bijvoorbeeld een gsm en zo informatie over de gebruiker wordt uitgelezen wanneer hij een bepaald punt voorbij komt. Toch voegt het Legal IST project hieraan toe dat wel onderzocht moet worden of bijkomende bescherming vereist is, daar ook RFID toelaat om personen te lokaliseren[35].

Omdat de meeste argumenten wijzen op een niet- of slechts beperkte toepasselijkheid van de richtlijn elektronische handel op RFID, laat ik ze verder buiten beschouwing.

3.3. PRIVACYBESCHERMING BIJ RFID

Zoals we hierboven reeds hebben kunnen vaststellen, bestaat er wel degelijk een risico op privacyinbreuken indien onzorgvuldig of onrechtmatig gebruik gemaakt wordt van de RFID-technologie. Voornamelijk het recht op informationele zelfbeschikking is in gevaar door de enorme hoeveelheid persoonsgegevens die, eventueel zelfs heimelijk, verzameld kan worden. Deze massa aan gegevens kan gebruikt worden om burgers of consumenten te beïnvloeden en te controleren. Toch kunnen we niet elke toepassing van RFID over dezelfde kam scheren, er bestaan immers ook veel toepassingen die geen enkel risico voor de privacy vormen[36].

We bekijken achtereenvolgens welke wetgeving op de RFID-technologie reeds van toepassing is, welke maatregelen getroffen kunnen worden om het risico op schending van de privacy te verkleinen of te neutraliseren en welke initiatieven de betrokken sectoren reeds genomen hebben om de bescherming van de privacy te waarborgen.

Anoniem communiceren: van drukpers tot weblog, in *ITeR Nationaal Programma Informatietechnologie en Recht,* Den Haag, SDU, 2006, 182-190.

[33] ECP.NL, *Privacyrechtelijke aspecten van RFID*, Efficiënta Offsetdrukkerij BV, 2005, 28-29.

[34] Communication from the commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, *Radio Frequency Identification (RFID) in Europe: steps towards a policy framework*, 2007, http://ec.europa.eu/information_society/policy/rfid/doc/rfid_en.pdf, laatst geconsulteerd op 7 mei 2007, 6.

[35] Legal IST Project, *Report on additional legal issues*, 2006, http://www.ve-forum.org/projects/P1507/D15%20Report%20on%20Additional%20Legal%20Issues%20-%20final%20version.pdf, laatst geconsuleerd op 5 mei 2007, 49.

[36] ECP.NL, *o.c.*, 22.

3.3.1. Privacy beschermende wetgeving van toepassing op de RFID-technologie

België, zoals de meeste andere lidstaten van de EU, heeft geen algemene "*Wet op de Privacy*". Hoewel beiden onder de noemer privacy vallen en niet steeds volledig van elkaar afgescheiden kunnen worden, zal ik hieronder toch een onderscheid maken tussen bescherming van de persoonlijke levenssfeer enerzijds en de bescherming van persoonsgegevens anderzijds. De bescherming van de persoonlijke levenssfeer behandel ik slechts kort, daar de grootste vragen rijzen rond de bescherming van persoonsgegevens[37].

3.3.1.1. Bescherming van de persoonlijke levenssfeer

Aandacht moet in dit verband geschonken worden aan het EVRM. Echte problemen zijn er tot nu toe niet geweest i.v.m. de toepassing van art 8 EVRM op nieuwe technologieën, maar toch blijkt uit de rechtspraak van het EHRM dat de beoordeling van privacyschendingen niet altijd even duidelijk was[38].

Het EHRM kijkt bij de beoordeling van een vermeende schending steeds naar ten eerste de aard van de informatie en ten tweede de mate van intimiteit. Niet alle persoongegevens worden immers evenwaardig beschermd. In tegenstelling tot wat het gegevensbeschermingsrecht doet, maakt het EHRM dus wel onderscheid tussen privacygevoelige en niet-privacygevoelige persoonsgegevens.

Daarnaast maakt het EHRM bij de beoordeling van een vermeende schending ook gebruik van de vanuit Amerika overgevlogen leer van de *reasonable expectation of privacy* die in 1967 door Justice Harlan werd geïntroduceerd[39]. Volgens Harlan moest de privacy enkel beschermd worden indien men daartoe een daadwerkelijke verwachting had én deze verwachting door de maatschappij ook als redelijk werd beschouwd. Er moet echter op gewezen worden dat het concept *reasonable expectation of privacy* niet volledig gelijk ingevuld wordt in Europa en de VS. Zo zal het EHRM, in tegenstelling tot het US Supreme Court, het concept enkel toepassen wanneer het gaat om publieke privacy. Dat komt o.a. doordat de privacybescherming die aan de Amerikaanse burgers geboden wordt minder ruim is dan de bescherming geboden door artikel 8 EVRM. Daarnaast lijkt het EHRM na de arresten *Ludi vs. Zwitserland*[40] en *Halford vs. het Verenigd Koninkrijk*[41] te hebben ingezien dat

[37] Die mening is ook de auteur van het Legal IST Project toegedaan, 10; P. DE HERT, *Privacy en persoonsgegevens*, Brussel, Politeia, 2004, Afl. 12, titel I, 152-155 en 157-160.
[38] P. DE HERT, *o.c.*, 80-89.
[39] in het bekende arrest *Katz vs. United States* gewezen door het U.S. Supreme Court.
[40] Lüdi v Switzerland, *EHRM* 15 juni 1992, Site ECHR, http://cmiskp.echr.coe.int/tkp197/view.asp?item=27&portal=hbkm&action=html&highlight=&sessionid=10078018&skin=hudoc-en, laatst geconsulteerd op 10 mei 2007; Zie ook R. LOERMANS, "Privacycolloquium 'Reasonable expectations of privacy'", *P&I*, 2004, nr. 4, 161.
[41] Halford v United Kingdom, *EHRM* 25 juni 1997, Site ECHR, http://cmiskp.echr.coe.int/tkp197/view.asp?item=1&portal=hbkm&action=html&highlight=&sessionid=10078018&skin=hudoc-en, laatst geconsulteerd op 10 mei 2007; Zie ook R. LOERMANS,

een onverkorte toepassing van het Amerikaanse *reasonable expectation of privacy*-concept zou leiden tot een lager beschermingsniveau in Europa. Toch heeft de nuancering van het concept niet kunnen verhinderen dat steeds meer inbreuken op de privacy getolereerd worden naarmate de technologie zich verder ontwikkelt[42]. Dat is bijvoorbeeld ook het geval geweest met het cameratoezicht.
Het EHRM oordeelde dat indien camerabeelden werden gemaakt op een publieke plaats in een situatie waarin de persoon wist dat hij gefilmd kon worden, hij zich niet op het recht op privacy kan beroepen. Hoewel het zover nog niet is, zou een analoge redenering gemaakt kunnen worden om RFID toepassingen te rechtvaardigen. Indien een persoon zich op een publieke plaats bevindt en weet dat hij gevolgd kan worden d.m.v. radiosignalen, zou hij, naar analogie artikel 8 EVRM niet meer kunnen gebruiken[43].
Het RFID-surveillancesysteem gaat zelfs nog een stapje verder. D.m.v. één enkele chip kan een consument gevolgd worden in al zijn gedragingen. Technisch gezien is het immers mogelijk d.m.v. één RFID-chip een consument te volgen over de hele wereld. Realistischer echter is het volgen van consumenten doorheen een winkel of van werknemers op hun werkvloer[44]. Of dit getolereerd zal worden is moeilijk te voorspellen, maar het staat vast dat het een gevoelige kwestie blijft. Zorgvuldigheid en terughoudendheid lijken dus in ieder geval gepast, zeker wanneer verschillende surveillance-infrastructuren zoals RFID, GPS en CCTV-systemen aan elkaar gekoppeld worden.

3.3.1.2. Bescherming van persoonsgegevens

Veel belangrijker i.v.m. de RFID-technologie dan de bescherming van de persoonlijke levenssfeer lijkt de bescherming van persoonsgegevens te zullen worden. We moeten dan ook eerst nagaan of en in hoeverre de gegevens verzameld d.m.v. RFID-toepassingen onder de noemer *persoonsgegeven* vallen. Daarna bekijk ik welke bescherming de Belgische wet en de Europese richtlijn bieden.

3.3.1.2.1. Het begrip persoonsgegeven

Het begrip persoonsgegeven wordt in artikel 1 van de Wet van 11 december 1998 gedefinieerd als "*iedere informatie betreffende een geïdentificeerde of identificeerbare natuurlijke persoon*". Dat heeft tot gevolg dat zowel tekst, beeld, geluid alsook de radiogolven gebruikt door RFID de wet vallen, althans indien ze herleidbaar zijn tot geïdentificeerde of identificeerbare personen. Een

---

l.c., 161.
[42] R. LOERMANS, *l.c.*, 159 en 161-162.
[43] P. DE HERT, *Privacy en persoonsgegevens*, Brussel, Politeia, 2004, Afl. 12, Titel I, 52-55 en 143-163; R. LOERMANS, "Privacycolloquium Reasonable expectations of privacy", *P&I*, 2004, nr. 4, 159-162; Supreme Court, arrest United States/Miller, 425 US, 1976, 435 en 440; P.G. en J.H. vs. Verenigd Koninkrijk, *EHRM,* 25 september 2001, nr. 4478/98.
[44] P. DE HERT, *o.c.*, 158-161.

persoon is identificeerbaar van zodra, zonder onredelijke moeite, achterhaald kan worden op wie de gegevens betrekking hebben. Anonieme gegevens vallen dus niet onder de wet, althans voor zover niemand de identiteit van de betrokkenen nog kan achterhalen. Deze definitie heeft grote gevolgen voor de RFID-technologie[45].

Wanneer d.m.v. de RFID-technologie gegevens als de naam, het adres en de geboortedatum, maar ook telefoon- of rijksregisternummers, gekoppeld kunnen worden aan een individu zal de Wet op de bescherming van persoonsgegevens nageleefd moeten worden. Het kan zijn dat zulke gegevens zelf opgeslagen liggen in een RFID-tag. Wanneer deze tag uitgelezen wordt, is er uiteraard sprake van een verwerking van persoonsgegevens. De meeste RFID-tags zullen echter zelf geen persoonsgegevens bevatten, maar enkel een unieke code. Indien deze code echter d.m.v. zogenaamde *middleware*, een achterliggende ICT-infrastructuur, gekoppeld kan worden aan persoonsgegevens, is evenzeer sprake van een verwerking. Hetzelfde geldt wanneer men camerabeelden van een consument kan koppelen aan identificerende informatie uit een RFID-chip. Er is echter nog meer. Wanneer de gegevens niet rechtstreeks identificerend zijn, maar d.m.v. nadere stappen in verband kunnen gebracht worden met een bepaalde persoon bijvoorbeeld door koppeling aan gegevens van een bankkaart, kredietkaart, factuur maar ook van een klantenkaart, zullen ook deze onder de wet vallen. In dit laatste geval moet rekening gehouden worden met de middelen die de verantwoordelijke van de verwerking kan of zal inzetten om de persoon te identificeren zoals bijvoorbeeld zijn bijzondere expertise en technische faciliteiten[46].

Ook de Artikel 29 Werkgroep heeft erkend dat in de drie hierboven beschreven gevallen aan de waarborgen ter bescherming van persoonsgegevens moet worden voldaan. Ik zet ze nog even op een rijtje:

- Ten eerste wanneer de RFID-tag zelf persoonsgegevens bevat
- Ten tweede wanneer de RFID-tag zelf geen persoonsgegevens bevat, maar de informatie uit de RFID-tag gekoppeld kan worden aan identificerende gegevens
- Ten derde wanneer RFID gebruikt wordt om individuele bewegingen te volgen en dit omdat de hoeveelheid verzamelde gegevens zo groot kan zijn dat de waarde ervan meer is dan de som van de afzonderlijke gegevens[47].

---

[45] Legal IST Project, *Report on additional legal issues*, 2006, http://www.ve-forum.org/projects/P1507/D15%20Report%20on%20Additional%20Legal%20Issues%20-%20final%20version.pdf, laatst geconsulteerd op 5 mei 2007, 48-49.

[46] ECP.NL, *Privacyrechtelijke aspecten van RFID*, Efficiënta Offsetdrukkerij BV, 2005, 22-24; X, "RFID en de bescherming van persoonsgegevens", *Computerrecht*, 2005, 109; P. DE HERT en D. PISSOORT, *Privacy en Persoonsgegevens*, 2005, Afl. 16, Titel II, 57-59.

[47] De Artikel 29 Werkgroep is een onafhankelijk overleg- en adviesorgaan van de nationale toezichthouders op gegevensbescherming die binnen de lidstaten werden opgericht n.a.v. de Data Protection Richtlijn. De werkgroep dankt haar naam aan artikel 29 van die richtlijn. Op 19 januari 2005 heeft de Werkgroep een Working document gepubliceerd over de gegevensbescherming bij gebruik van RFID: *Working document on data protection issues related to RFID technology*, 2005, website Europese regelgeving, http://www.europa.eu.int/comm/internal-

Hoewel dus algemeen erkend wordt dat niet elke toepassing van RFID een risico op schending van de privacy met zich meebrengt, bestaat er toch het idee om elk gegeven opgeslagen op een RFID-chip automatisch als een persoonsgegeven te beschouwen. Het voorstel daartoe werd o.a. geopperd door de Franse toezichthouder op de bescherming van persoonsgegevens, de CNIL, en de Nederlandse organisatie voor digitale burgerrechten Bits of Freedom. Het Nederlandse E-Commerce Platform (ECP.NL) wijst er echter op dat gezien de technische omstandigheid dat een RFID-tag automatisch communiceert met een reader op het moment dat deze binnen het stralingsveld daarvan komt, zelfs het gewoon uitlezen van een RFID-tag als een verwerking van persoonsgegevens moet worden beschouwd. Dat zou leiden tot onwerkbare situaties en volgens het ECP.NL zou dat zelfs tot verwatering van de kracht van de gegevensbeschermingswetgeving kunnen leiden[48].

3.3.1.2.2 .Bescherming van persoonsgegevens

Om persoonsgegevens rechtmatig te verwerken moeten voornamelijk de volgende elementen in rekening worden gebracht: de naleving van het finaliteitsbeginsel, het toetsen van elke verwerking aan de toelaatbaarheidscriteria en de eisen betreffende de vertrouwelijkheid en beveiliging. Naast deze algemene waarborgen bevat de wet ook nog een aantal rechten voor de betrokkenen die gerespecteerd moeten worden door de verantwoordelijke voor de verwerking.

1) Algemene waarborgen

(i) Finaliteitsbeginsel

Vóór elke verwerking moet men een duidelijk omschreven en gerechtvaardigd doel aanduiden waarvoor de verwerking van de persoonsgegevens zal gebruikt worden[49]. Naderhand mogen de gegevens niet gebruikt worden op een andere dan met dat doel verenigbare wijze, en enkel voor het oorspronkelijk aangeduide doel. Bij de verwerking moeten bijgevolg eerlijkheid, transparantie en oprechtheid voorop staan.

Het finaliteitsbeginsel impliceert daarnaast ook dat men enkel deze gegevens mag verzamelen die toereikend, relevant en noodzakelijk zijn én dat deze gegevens ook niet langer dan nodig bewaard mogen worden[50].

_market/privacy/workinggroup/wp/2005/wpdocs05_en.htm., laatst geconsulteerd op 24 februari 2007, 5-8; Zie ook X, "RFID en de bescherming van persoonsgegevens", *Computerrecht*, 2005, 109; J. KOHNSTAMM en M. FONTEIN, "Interpretatie en harmonisatie: het werkprogramma van de Artikel 29-werkgroep voor 2006 en 2007", 2006, *P&I*, afl. 3, 127-128.

[48] ECP.NL, *o.c.*, 22-24.

[49] Zie art 6 Richtlijn 95/46 en art 4 Wet verwerking persoonsgegevens.

[50] J. DUMORTIER, "Privacybescherming bij de verwerking van persoonsgegevens", in *Mediarecht, Telecommunicatie en telematica*, Mechelen, Kluwer, 1999, Afl. 12, 66-68; P. DE HERT en D. PISSOORT, *Privacy en Persoonsgegevens*, 2005, Afl. 16, Titel II, 14-15 en 17-18.

Hierbij is het vooral belangrijk te beseffen dat de meeste RFID-systemen tot eindeloze toepassingen kunnen leiden of zoals het ECP.NL het formuleerde: "*het is het probleem van het hellend vlak*". De ene toepassing ontlokt de andere. Het ECP.NL geeft in haar verslag ook een duidelijk voorbeeld dat ik hier graag over neem. Auto's kunnen uitgerust worden met een passieve tag die functioneert als een digitaal nummerbord. Deze tag kan tot een afstand van vijf meter uitgelezen worden, zelfs bij een snelheid van 200km/u. De tags kunnen bijgevolg probleemloos gebruikt worden voor tolheffingen, snelheidcontroles en zelfs als parkeermeter. Secundair echter zou bijvoorbeeld ook een tankstation een beroep kunnen doen op de tag om het wegrijden zonder betalen te bestrijden en zo verder[51].

(ii) Toelaatbaarheidstoetsing

Vóór elke verwerking van persoonsgegevens moet tevens nagegaan worden of ze toelaatbaar is, of er m.a.w. een rechtvaardigende rechtsgrond bestaat voor de verwerking[52]. In verband met RFID zal de enige mogelijke rechtsgrond in vele gevallen bestaan uit de toestemming van de betrokken persoon. Deze toestemming is enkel geldig indien ze vrij, ondubbelzinnig én geïnformeerd werd gegeven. Dat impliceert ten eerste dat de aanvaarding niet mag afgedwongen zijn, maar bijvoorbeeld ook niet mag afgekocht zijn. Dat kan wel het geval zijn wanneer een supermarkt of enige andere winkel haar klantenkaarten uitrust met een RFID-chip. Ten tweede meent de Europese Commissie dat het geven van een geïnformeerde toestemming op dit ogenblik nog onmogelijk is enkel en alleen omdat er te weinig informatie beschikbaar is over de risico's i.v.m. RFID[53].

Aangezien de betrokkene zijn toestemming steeds kan intrekken, moet er daarenboven een mogelijkheid bestaan om de verzameling van gegevens te stoppen en zelfs om de reeds verzamelde gegevens te (doen) wissen, wanneer de enige rechtsgrond voor de verzameling van de gegevens de toestemming van de consument is. Dit komt bijvoorbeeld onder druk te staan wanneer RFID-implantaten gebruikt worden zoals in de Baja Beach Clubs. Er zal weliswaar voldaan zijn aan de vereiste van vrije toestemming van de klant om de chip in te laten planten, maar kan zijn toestemming ook eenvoudig worden ingetrokken? Kan de chip even eenvoudig worden verwijderd als dat zij werd ingeplant of is hiervoor een operatie vereist?

Een andere rechtvaardigingsgrond, die bijvoorbeeld bij medische toepassingen van RFID of bij de bewaking van gevangenen d.m.v. RFID kan bestaan, is de

[51] ECP.NL, *Privacyrechtelijke aspecten van RFID*, Efficiënta Offsetdrukkerij BV, 2005, 34.
[52] Zie art 7 Richtlijn 95/46 en art 5 Wet verwerking persoonsgegevens; J. DUMORTIER, *o.c.*, 68-69.
[53] Communication from the commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, *Radio Frequency Identification (RFID) in Europe: steps towards a policy framework*, 2007, http://ec.europa.eu/information_society/policy/rfid/doc/rfid_en.pdf, laatst geconsulteerd op 7 mei 2007, 7.

vrijwaring van een vitaal belang voor de betrokkene of voor de maatschappij. Men rust bijvoorbeeld chirurgische instrumenten uit met een chip om het risico op achtergebleven instrumenten na een operatie te verminderen. In dit geval kan men argumenteren dat het gebruik ervan in het belang van de patiënt zelf is. Toch zal deze rechtvaardigingsgrond slechts in zeer uitzonderlijke gevallen gebruikt kunnen worden, te meer omdat ook in deze gevallen steeds de noodzakelijkheid, proportionaliteit en het respect voor de menselijke waardigheid zal moeten onderzocht worden[54].

In dit verband moet ook melding gemaakt worden van de extra beschermingen die voorzien zijn voor een aantal specifieke categorieën van gegevens. Het gaat met name om gevoelige, gerechtelijke en medische gegevens zoals bijvoorbeeld gegevens over ras, politieke opvattingen, lidmaatschap van een vakvereniging, het seksuele leven, verdenkingen, vervolgingen en het medisch verleden. In deze gevallen is de verzameling van gegevens in beginsel verboden, maar de wet bevat een hele reeks uitzonderingen[55]. Daarop ga ik hier echter niet verder in.

(iii) Veiligheid en vertrouwelijkheid

Ten eerste vereist de wet dat de relatie tussen de verantwoordelijke voor de verwerking en de verwerker waarop hij een beroep doet, schriftelijk geregeld wordt. In dat schriftelijk contract moet o.a. de aansprakelijkheid uitdrukkelijk aan bod komen. Ten tweede heeft de verantwoordelijke voor de verwerking een aantal verplichtingen t.a.v. het personeel dat toegang krijgt tot de gegevens. Ten slotte vereist de wet ook dat er voldoende technische en organisatorische maatregelen genomen worden om de persoonsgegevens te beveiligen tegen onrechtmatige toegang, wijziging, verlies of vernietiging. Daarbij moet/mag rekening gehouden worden met de stand van de techniek, de kosten van tenuitvoerlegging, de potentiële risico's en de aard van de gegevens[56].

Uit het Working document van de Artikel 29 Werkgroep blijkt dat zij er van overtuigd zijn dat de techniek zelf een belangrijke rol moet spelen bij de bescherming van gegevens verkregen d.m.v. RFID-technologie. Zij stellen dat er ten eerste standaardiseringinitiatieven moeten komen voor zowel de RFID-tag, -readers als -toepassingen. Dat zou kunnen helpen bij de beperking van de hoeveelheid persoonsgegevens die verzameld wordt. Ten tweede moet er gebruik gemaakt worden van ingebouwde technische codering. Dat zou kunnen voorkomen dat onbevoegde personen kennis krijgen van de gegevens en er misbruik van maken. Dat zal bijvoorbeeld essentieel zijn wanneer RFID-

[54] Legal IST Project, *Report on additional legal issues*, 2006, http://www.ve-forum.org/projects/P1507/D15%20Report%20on%20Additional%20Legal%20Issues%20-%20final%20version.pdf, laatst geconsuleerd op 5 mei 2007.

[55] J. DUMORTIER, "Privacybescherming bij de verwerking van persoonsgegevens", in *Mediarecht, Telecommunicatie en telematica*, Mechelen, Kluwer, 1999, Afl. 12, 69.

[56] Zie art 16-17 Richtlijn 95/46 en art 16 Wet verwerking persoonsgegevens; J. DUMORTIER, *o.c.*, 73.

tags in ziekenhuizen gebruikt worden ter identificatie van patiënten en tegelijkertijd de tag gevoelige medische informatie bevat. De werkgroep wijst er dan ook op dat hoewel de gebruikers van RFID-toepassingen verantwoordelijk zijn voor de verwerking van persoonsgegevens, ook de ontwikkelaars van de RFID-technologie en de organisaties voor standaardisering een verantwoordelijkheid dragen[57].

2) Rechten voor de betrokkenen

(i) Recht op informatie en het recht om vragen te stellen

Persoonsgegevens mogen niet verwerkt worden zonder medeweten van de betrokkenen. Aan de betrokkenen moet steeds worden meegedeeld wie verantwoordelijk is voor de verwerking en waarvoor de gegevens gebruikt zullen worden. Dat is ook vereist wanneer de gegevens niet rechtstreeks bij de betrokkenen zelf werden ingewonnen. Iedereen heeft daarenboven het recht om aan iedere verantwoordelijke voor een verwerking te vragen of hij al dan niet gegevens over hem bezit en waarvoor hij deze gebruikt[58].

In winkels heeft dit bijvoorbeeld tot gevolg dat de consument op de hoogte moet worden gebracht van de aanwezigheid van RFID-tags op producten en de aanwezigheid van RFID-lezers in de winkel, maar ook van de informatie die d.m.v. deze technologie over hem of haar verzameld kan worden én over het feit dat dit automatisch kan gebeuren.

Daarnaast moet de consument ook op de hoogte worden gebracht van de intentie die de winkelier heeft m.b.t. de verzamelde informatie. Hij moet ingelicht worden over het doel van de verzameling en over welke partijen kennis zullen kunnen krijgen van de verzamelde gegevens. Het finaliteitsbeginsel vereist daarenboven dat dit op een duidelijke en voor de consument begrijpbare manier gebeurt.

Om aan dit recht op informatie te voldoen stelt de Artikel 29 Werkgroep ten eerste voor om een pictogram te ontwerpen dat verplicht en goed zichtbaar aangebracht moet worden op elk product dat RFID-technologie bevat. Ten tweede stelt zij ook voor regelingen op te stellen i.v.m. de *real time activation* van RFID-toepassingen. Op dit tweede voorstel kom ik later nog terug[59].

Meer algemeen geldt daarenboven ook hier dat een goed geïnformeerde consument er twee waard is. Het is niet enkel belangrijk de consument te informeren over het gebruik van de RFID-technologie, maar ook over de werking ervan. RFID technologie is nog niet erg bekend bij het grote publiek

---

[57] Article 29 Working Party, *Working document on data protection issues related to RFID technology*, 2005, website Europese regelgeving, http://www.europa.eu.int/comm/internal-_market/privacy/workinggroup/wp/2005/wpdocs05_en.htm., laatst geconsulteerd op 24 februari 2007, 9-12.

[58] Zie art 10-11 Richtlijn 95/46 en art 9-10 Wet verwerking persoonsgegevens; J. DUMORTIER, "Privacybescherming bij de verwerking van persoonsgegevens", in *Mediarecht, Telecommunicatie en telematica*, Mechelen, Kluwer, 1999, Afl. 12, 76.

[59] Article 29 Working Party, *o.c.*, 11-16.

en bijgevolg is een open houding van de industrie tegenover de consument zeer belangrijk. Ook daar kom ik i.v.m. *policies* van de bedrijfswereld nog op terug.

(ii) Recht op toegang, correctie en verzet

Het recht op toegang impliceert dat iedere persoon van wie gegevens worden verwerkt het recht heeft om van de verwerkte gegevens een afschrift te krijgen en te weten waar deze gegevens verzameld werden[60]. Elke betrokkene moet daarenboven, in navolging van het recht op correctie, de mogelijkheid krijgen om zijn gegevens kosteloos te (doen) verbeteren en om onvolledige, irrelevante of verboden gegevens te (doen) wissen[61]. Ten derde heeft men ook het recht om zich te verzetten tegen de opname van zijn gegevens in een bestand[62].

Voor wat dit laatste recht betreft, moet wel een onderscheid gemaakt worden tussen de gegevens verzameld om marketingredenen en de gegevens verzameld om andere dan marketingredenen. Worden gegevens verzameld om marketingredenen, kan met steeds, ook zonder enige motivatie, verzet aantekenen. Worden de gegevens echter om andere dan marketingredenen verzameld, moet men er een zwaarwichtige reden toe hebben. De wet bevat echter geen definitie van wat wel en wat niet onder marketing valt. Aangenomen wordt dat het zowel gaat om commerciële direct marketing als op individuele personen gerichte acties voor caritatieve, electorale en andere doeleinden.

Het recht op toegang en correctie impliceren dat elk individu alle over hem verzamelde gegevens moet kunnen kennen. Wordt in een winkel bijgehouden welke consument wat koopt, moet de consument tot die bestanden toegang krijgen. Bevat de chip in zijn klantenkaart persoonlijke informatie, moet hij kunnen weten welke informatie precies en moet hij gemakkelijk kunnen (laten) verbeteren.

Hoewel het recht op toegang en correctie op het eerste zicht heel eenvoudig lijken, laten zij i.v.m. RFID toch een aantal problemen rijzen. Dat heeft ook de Artikel 29 Werkgroep ondervonden. Ten eerste heeft men, om toegang te krijgen tot de informatie opgeslagen op de RFID-tag of –chip zelf een speciale RFID-reader nodig, die vanzelfsprekend niet iedereen heeft. Zelfs indien iedereen toch de inhoud van de RFID-tag of –chip zou kunnen lezen is het nog niet zeker dat hij de inhoud ervan ook kan begrijpen. Een tag of chip zal immers vaak slechts een code bevatten. Wat die code betekent, kan dan maar achterhaald worden door de inschakeling van *middleware* waartoe slechts een zeer beperkt aantal mensen toegang hebben. Het standaardiseren van de codes

[60] Zie art 12 Richtlijn 95/46 en art 10 Wet verwerking persoonsgegevens.
[61] Zie art 12 Wet verwerking persoonsgegevens.
[62] Zie art 14 Richtlijn 95/46 en art 12 Wet verwerking persoonsgegevens; J. DUMORTIER, "Privacybescherming bij de verwerking van persoonsgegevens", in *Mediarecht, Telecommunicatie en telematica*, Mechelen, Kluwer, 1999, Afl. 12, 76-78.

zou een oplossing kunnen zijn, maar dat brengt dan weer een verhoging van het risico op inbreuken door onbevoegden met zich mee.

Wat het stopzetten van het verspreiden van gegevens betreft heeft de Artikel 29 Werkgroep wel een oplossing. Technisch gezien is het mogelijk om alle gegevens opgeslagen op een tag of chip automatisch te wissen wanneer men bijvoorbeeld een winkel verlaat. Men kan hiervoor een zogenaamd "*kill-command*" gebruiken of men kan de informatie op de RFID-tag overschrijven met nullen (al lijkt deze laatste oplossing toch niet alle sporen uit te wissen[63]). De tag kan dan ofwel permanent ofwel enkel tijdelijk gedeactiveerd worden. Voor tijdelijke deactivatie stelt de werkgroep een softwareslot voor. Door te voorzien in een mechanisme waarmee de betrokkene kan voorkomen dat de RFID-toepassing verder informatie over hem verspreidt, komt men ook tegemoet aan het probleem van het verdwijnen van de enige rechtsgrond bij intrekking van de toestemming. Daarbij zal echter enkel aan de vereisten van de gegevensbeschermingswet voldaan worden wanneer deze technische oplossing zo wordt ontwikkeld dat ze ook voor elke consument-betrokkene eenvoudig toe te passen is.

De werkgroep vermeldt hierbij evenwel meteen dat door alle RFID-tags automatisch uit te schakelen de voordelen van het blijvend gebruik van de RFID-toepassing buiten de winkel verloren gaat. Zo valt bijvoorbeeld ook het voordeel van RFID voor garanties of diensten na verkoop weg. Bijkomend probleem is dat consumenten moeilijk kunnen controleren of de tag wel degelijk gestopt is met het verspreiden van gegevens[64].

Een andere slechts beperkt bruikbare oplossing tegen het ongewenst uitlezen van RFID-tags of –chips is het omwikkelen van het product met aluminiumfolie. Zo kan men bijvoorbeeld in paspoorten die RFID-tags bevatten een metaallaagje verwerken waardoor deze niet te pas en te onpas kunnen uitgelezen worden. Ook in handtassen zou men zo een laagje kunnen verwerken om te voorkomen dat RFID-signalen van bankbriefjes ongewenst gelezen worden. Toch maakt even logisch nadenken al meteen duidelijk dat dit niet voor elke RFID-toepassing een geschikte oplossing kan bieden. Zo kan men moeilijk zijn horloge met zilverpapier gaan omwikkelen. Daarenboven doet dit ten eerste niets af aan het feit dat RFID-chips zodanig klein kunnen zijn dat ze met het blote oog amper te zien zijn, of dat de betrokkene gewoon niet weet dat hij RFID-signalen uitzendt en biedt het ten tweede ook geen bescherming tegen de actieve RFID-chips die wel door metaal gelezen kunnen worden[65].

---

[63] Zo zal men nog steeds de lengte van de oorspronkelijke code kunnen zien en kan, indien deze lengte slechts uitzonderlijk wordt gebruikt, daar nog steeds waardevolle informatie uit worden afgeleid.

[64] Article 29 Working Party, *o.c.*, 15-16.

[65] Daarnaast moet ook nog vermelding gemaakt worden van "*blocker tags*" en het "*User-model-solution*". Blocker tags zijn tags die andere tags simuleert en die de informatie uit andere tags in de war stuurt wanneer consumenten de blocker bij zich dragen. De User-model-solution gaat er van uit dat gebruikers volledig zelf controle krijgen over de RFID-tags doordat deze niet automatisch en autonoom kunnen werken, maar steeds door een individu gehanteerd moeten worden. Toch

Het recht op verzet lijkt dan weer een keuzerecht te impliceren voor de consument in geval we te maken hebben met marketingdoeleinden. De consument zou de volledige vrijheid moeten hebben om ervoor te kiezen geen gebruik te maken van RFID-toepassingen. Omdat de RFID-toepassingen automatisch werken zou er een recht op het verwijderen van de RFID-technologie moeten bestaan. Het verwijderen of uitschakelen van de RFID-toepassing moet daarenboven eenvoudig zijn. De consument zal immers steeds een afweging maken tussen de voor- en nadelen van de uitschakeling. Indien de nadelen van de uitschakeling niet opwegen tegen de voordelen van het actief laten, zal de consument zijn keuze snel gemaakt zijn.

Concreet komt dit er op neer dat hij eventuele RFID-tags of –chips te allen tijde eenvoudig uit bijvoorbeeld zijn kleding, horloge of exclusieve handtas, moet kunnen verwijderen. Maar bijvoorbeeld ook het aanbieden van klantenkaarten enkel mét RFID-chip kan een inbreuk vormen op de keuzevrijheid van de consument. Immers indien men enkel d.m.v. het houden van een klantenkaart bepaalde kortingen kan krijgen en de winkel geeft enkel klantenkaarten met RFID-chips uit, dan is de keuze van de consument niet meer vrij. Daarom zouden ook bijvoorbeeld commerciële garantiebepalingen niet afhankelijk gesteld mogen worden van het actief laten van de RFID-technologie. Hetzelfde geldt voor uitbaters van openbaar vervoer zoals bijvoorbeeld metrosystemen die gebruik maken van RFID. Er bestaan bij de huidige proefprojecten meestal twee soorten kaarten: een persoonsgebonden kaart en een anonieme kaart. Echter omdat de persoonsgebonden kaart voor de uitbater meer voordelen biedt - hij kan het reisgedrag dan immers beter volgen - maakt hij het reizen met een persoonsgebonden kaart goedkoper of vergemakkelijkt hij bijvoorbeeld het tegoedbeheer. Bijgevolg zal de consument gauw geneigd zijn toch maar een persoonsgebonden kaart te kiezen.

Een persoon die kiest voor de verwijdering of uitschakeling van de RFID-chip zou m.a.w. nooit benadeeld of "gestraft" mogen worden. Indien aan deze keuzevrijheid niet tegemoet gekomen wordt, ontstaat er een vorm van systeemdwang. De consument die zich toegang wil verschaffen tot een winkel of de metro moet de gevolgen van de nieuwe RFID-toepassingen verplicht ondergaan. Dat kan dan weer tot gevolg hebben dat de vaak enige rechtsgrond voor het rechtsgeldig verkrijgen en verwerken van persoonsgegevens, namelijk de toestemming van de consument, wegvalt. De verwerking wordt bijgevolg onrechtmatig[66].

3.3.2. Regelgevende initiatieven i.v.m. RFID

---

kunnen ook deze nieuwe uitvindingen geen volledige bescherming bieden. Zie Legal IST Project, *Report on additional legal issues*, 2006, http://www.ve-forum.org/projects/P1507/D15%20Report%20on%20Additional%20Legal%20Issues%20-%20final%20version.pdf, laatst geconsuleerd op 5 mei 2007, 54; Article 29 Working Party, *o.c.*,16-17.

[66] M. VAN LIESHOUT, *Naar een internet van kleine dingen*, gepubliceerd op de website van het Rathenau Instituut, http://www.e-jure.nl, laatst geconsulteerd op 14 april 2006, 5.

Er bestaan naast de wetgeving reeds verschillende regelgevende initiatieven op het gebied van privacy in het algemeen en RFID in het bijzonder. Hoewel deze regelgevingen niet de status hebben van wetgeving kunnen zij toch van groot belang zijn.

Belangrijke algemene initiatieven zijn de opstelling van de Fair Information Practice Principles[67] en de OECD Privacy Guidelines[68] geweest. Op deze algemene principes die voornamelijk de bescherming van persoonsgegevens tegen misbruiken allerhande tot doel hebben, zijn de Europese wetgevingen geënt. Reeds in de jaren '80 besefte men dat een aantal veiligheidmechanismen ingebouwd moesten worden zoals een verbod op geheime verwerking en bescherming tegen ongeoorloofde toegang. Daarnaast werd voornamelijk gedrukt op de algemene zorgvuldigheidsplicht die ook bij de verwerking van persoonsgegevens niet genegeerd mag worden. Wat wel opvalt, is dat in tegenstelling tot de Europese Richtlijn van 1995, de OECD Privacy Guidelines een apart *Openness principle* bevatten. Er wordt m.a.w. harder gehamerd op een algemene openheid bij de ontwikkeling, toepassing en beleidsvorming op het gebied van verwerking van de persoonsgegevens. In verband met RFID is juist die openheid, zoals hierboven reeds aangeduid, één van de vragen van consumentenorganisaties, maar ook van de Europese Commissie.

Belangrijke initiatieven specifiek van toepassing op RFID-technologie zijn de RFID Bill of Rights, de EPC Guidelines, en de ICDPPC Resolution on Radio Frequency Identification.

3.3.2.1. De RFID Bill of Rights

Simon Garfinkel heeft zijn Bill of Rights opgesteld om de mogelijke risico's voor de privacy bij het gebruik van RFID aan te duiden en een raamwerk te creëren voor eventuele zelfregulerende initiatieven vanuit de bedrijfswereld waarin de rechten van de consument gewaarborgd blijven[69].

Ten eerste heeft de consument recht op informatie: hij moet in kennis gesteld worden van het feit dat een product uitgerust is met RFID-technologie en welke informatie deze bevat of hiermee verzameld kan worden en waarom dat zo is. Ten tweede duidt ook Garfinkel op het keuzerecht: de consument heeft het recht RFID-tags te kunnen verwijderen of te kunnen uitschakelen en de consument moet het recht hebben om gebruik te maken van diensten zonder RFID.

3.3.2.2. EPC guidelines

[67] Het is het US Department of Health dat de Fair Information Practice Principles heeft geïntroduceerd en gepubliceerd.

[68] De OECD Privacy Guidelines zijn in de jaren '80 opgesteld door de OESO (Organisatie voor Economische en Sociale Ontwikkeling); zie ook M. VAN LIESHOUT, *o.c.*, 8.

[69] Zie ook ECP.NL, *Privacyrechtelijke aspecten van RFID*, Efficiënta Offsetdrukkerij BV, 2005, 52.

EPCglobal Organisatie stelt zichzelf op haar website voor als de leidinggevende organisatie die op vraag van de industrie standaarden opstelt i.v.m. de Electronic Product Code (EPC)[70]. De EPC guidelines zijn voornamelijk bedoeld om het vertrouwen in het gebruik van EPC en het EPCnetwork te stimuleren. Daarbij moet steeds in het achterhoofd gehouden worden dat de EPCglobal Organisatie gesponsord wordt door de industrie. Deze "*guidelines*" vormen dus één van die zelfregulerende initiatieven uit de bedrijfswereld waarvoor Garfinkel precies zijn Bill of Rights heeft opgesteld.
Sinds 1 januari 2005 hebben de gebruikers van EPC de wil uitgedrukt om d.m.v. vier basisprincipes rekening te houden met de bezorgdheden van consumenten over hun privacy bij het gebruikt van RFID. Ten eerste engageren ze zich tot het informeren van consumenten over het gebruik van RFID bijvoorbeeld door een symbool af te beelden op de verpakking of het product. Dit noemt men de *Consumer Notice*. Ten tweede zullen ze consumenten informeren over de mogelijkheid tot verwijdering of uitschakeling van de tags. Dit noemt men de *Consumer Choice*. Ten derde heeft men ook een *Consumer Education engagement* aangenomen. Men vindt dat consumenten snel en gemakkelijk duidelijke informatie moeten kunnen krijgen over het bestaan, gebruik en toekomstige ontwikkelingen van EPC. Ten slotte benadrukt de organisatie dat de EPC-technologie geen persoonsgegevens bevat en dat bestaande wetgevingen nageleefd moeten worden. Dit laatste engagement wordt aangeduid met de termen *Record Use, Retention and Security*.

Over het gebruik van EPC-systemen en zelfregulering daar rond heeft ook de Internationale Kamer van Koophandel in 2005 een advies gegeven. Het uitgangspunt daarin is dat een goede voorlichting essentieel is voor een eerlijk en verantwoord gebruik van de systemen. Indien bedrijven zelf *policies* opstellen, moeten ze deze ook publiek maken. Daarbij moet, zo zegt het de ICC uitdrukkelijk, ook rekening gehouden worden met deze consumenten die geen toegang tot het internet hebben. Ten slotte wijst men ook hier op de verplichte doelgebondenheid en het recht op informatie en keuzevrijheid van iedere consument[71].

3.3.2.3. De ICDPPC Resolution on Radio-Frequency Identification

In november 2003 werd the International Conference of Data Protection & Privacy Commissioners, een internationale conferentie over het verantwoord gebruik van RFID-technologie, georganiseerd. Op deze conferentie nam men een resolutie aan waarin men aandringt op zo veel mogelijk anonimisering van gegevens en de aandacht vestigt op de veiligheid bij de verwerking.
Ten eerste kwam men op de conferentie tot de conclusie dat elke

[70] Door middel van individuele codes die aan producten worden gegeven stelt men een EPCglobal Network in dat gebruikt kan worden om identificatiecodes uit RFID-tags en –chips een betekenis te geven.
[71] Zie ook ECP.NL, *o.c.*, 51-52; B. SCHERMER, "Big Brother in een kleine chip?", 2004, *JAVI* (Ned.), nr. 5, 162.

verantwoordelijke, alvorens over te gaan tot implementering van een RFID-systeem dat persoonsgegevens verwerkt, alle mogelijke alternatieven moet overwegen waarmee hetzelfde doel kan bereikt worden zonder verwerking van persoonsgegevens. Ten tweede wil men indien er toch persoonsgegevens worden verwerkt deze zo veel als mogelijk beschermen. Dat moet bereikt worden door een open en transparante houding van de verantwoordelijken, maar ook door strikt doelgebonden verwerking en door het steeds respecteren van de keuzevrijheid van ieder individu[72].

3.3.3. Toetsing van de regelgevende initiatieven aan de bestaande wetgeving

Ik heb de indruk dat in de Bill of Rights van Garfinkel enkel een aantal reeds bestaande rechten worden benadrukt, maar dan toegepast op RFID. Daarbij lijkt zijn interpretatie van de waarborgen overeen te komen met deze die door de rechtspraak en de rechtsleer gegeven wordt aan de waarborgen uit de richtlijn van 1995.

Voor wat het initiatief van EPC betreft denk ik dat er niet zozeer een probleem is van niet overeenstemming met de wetgeving, al had de Internationale Kamer van Koophandel wel enkele terechte opmerkingen, maar ligt het probleem eerder bij de vraag of deze policies volstaan. Die vraag behandel ik in het volgende hoofdstuk.

4. VOLSTAAT DE BESTAANDE WETGEVING?

4.1. DE ECONOMIE TEGENOVER HET ALGEMEEN WELBEHAGEN VAN HET INDIVIDU

Hierover zijn de meningen duidelijk verdeeld. Er moet voornamelijk een onderscheid gemaakt worden tussen de opinie van de bedrijfswereld zoals die van het E-Commerce Platform Nederland of ECP.NL, de opinie van de consumenten en privacyorganisaties zoals de Nederlandse organisatie Bits of Freedom en de opinie van de Europese Commissie, die deze twee probeert te verzoenen. Het ECP.NL formuleerde in 2005 een besluit over de privacyrechtelijke aspecten van RFID[73] waarin het o.a. antwoordde op de vraag of aanvullende wetgeving noodzakelijk is. Ook Bits of Freedom maakte oorspronkelijk deel uit van het forum, maar trok zich later terug omdat in het uiteindelijke besluit te weinig verplichtingen werden opgelegd aan de private sector en te veel ruimte werd gelaten voor misbruik van persoonsgegevens. De organisatie stelde zijn eigen Position Paper op[74].

Ook de bedrijfswereld erkent weliswaar meer en meer dat de consument

[72] ECP.NL, *o.c.*, 52.

[73] ECP.NL, Privacyrechtelijke aspecten van RFID, Efficiënta Offsetdrukkerij BV, 2005.

[74] S. VERHAEGH, *Bits of Freedom Positioning Paper*, Organisatie voor digitale burgerrechten, http://www.bof.nl/rfid/RFIDpositionpaper.html, laatst geconsulteerd 10 mei 2007.

rechten heeft, maar nooit zonder daaraan toe te voegen dat hij zelf ook een verantwoordelijkheid draagt. Toch erkende ook het ECP.NL dat een consument niet verantwoordelijk kan gesteld worden voor verspreiding van zijn eigen gegevens wanneer hij niet geïnformeerd wordt over de werking en het gebruik van de nieuwe technologie. Deze toenadering lijkt echter zijn oorzaak te hebben in eigenbelang. Ook de bedrijfswereld beseft immers dat de consument macht heeft en dat iedereen gebaat is bij een strenge handhaving en sanctionering van (zelf)regulering[75]. Dat laatste heeft ook de Europese Commissie benadruk in haar verslag over de ontwikkelingen i.v.m. RFID. Daarin zei ze dat "*with wider use, it becomes essential that the implementation of RFID takes place under a Legal framework that affords citizens effective safeguards for fundamental values, health, data protection and privacy*"[76].

Zowel de bedrijfswereld als de consumentenorganisaties lijken dus aan te voelen dat de bestaande wetgeving niet volstaat. Het verschil is echter dat consumentenorganisaties het uitdrukkelijk durven stellen terwijl de bedrijfswereld het subtieler aanpakt en bijvoorbeeld zegt dat de huidige gegevensbescherming wel volstaat, maar geconcretiseerd moet worden. Het valt daarbij op, maar moet natuurlijk niet verbazen, dat de bedrijfswereld pleit voor zelfregulering en sectorspecifieke reguleringen terwijl de consumentenorganisaties vooral de nadruk leggen op afdwingbare wettelijke waarborgen voor de consument[77]. Het ECP.NL stelt bijvoorbeeld voor een Model Code Privacy & RFID op te stellen in overleg tussen zowel aanbieders, gebruikers, consumenten, burgers als de overheid die als richtsnoer zal dienen voor sectorspecifieke gedragsregels. Zij wil zo veel als mogelijk verbodsbepalingen vermijden en opteren voor "mechanismen" die een onverantwoord gebruik van de RFID-technologie moeten voorkomen[78].

Bits of Freedom daarentegen meent dat alleen de invoering van een *opt-in* verplichting (of keuzevrijheid) consumenten kan beschermen tegen de heimelijke en ongewenste gevolgen van RFID[79]. Ook Wim Schreurs is van mening dat het afnemen van het keuzerecht een fundamenteel probleem is. Hij kan ermee leven dat we als burger geen inspraak hebben in de implementatie van de technologie in de maatschappij, maar het afnemen van het keuzerecht is een brug te ver. De maatschappij verplicht ons m.a.w. tot het gebruik van paspoorten uitgerust met RFID-tags, tot het aannemen van RFID-geld en tot

[75] ECP.NL, *o.c.*, 34-43.

[76] Communication from the commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, *Radio Frequency Identification (RFID) in Europe: steps towards a policy framework*, 2007, http://ec.europa.eu/information_society/policy/rfid/doc/rfid_en.pdf, laatst geconsulteerd op 7 mei 2007, 3.

[77] Zie o.a. RFID Position Statement of Consumer Privacy and Civil Liberties Organisation, http://www.privacyrights.org/ar/RFIDposition.htm, laatst geconsulteerd op 22 februari 2007; Projecten van Amerikaanse consumentenorganisatie CASPIAN opgericht door Katherine Albrecht, http://www.stoprfid.com en http://www.spychips.com.

[78] ECP.NL, *o.c.*, 44; Zie ook C. CUIJPERS (ed.), "RFID: 'geen paniekwetgeving'", *Computerrecht*, 2005, 289-290.

[79] Zie ook J. KURI, A. MEYER en P. SCHULER, "In het vizier", *c't*, 2004, nr. 5, 114.

het rijden met een met RFID uitgeruste auto, maar dat we zouden moeten aanvaarden gevolgd te worden in bijvoorbeeld onze winkelgewoontes is een brug te ver[80].

Het feit dat de bedrijfswereld opteert voor zelfregulering heeft ook te maken met de vrees voor een contraproductief effect van aanvullende wetgeving op de implementering van RFID. Deze bezorgdheid vinden we vanzelfsprekend terug in het besluit van ECP.NL, maar ook in opiniestukken van andere auteurs wordt dit gevaar erkend[81]. De RFID-industrie in Europa is vandaag immers al miljarden waard. De voordelen van RFID zijn zelfs op korte termijn zo groot, dat ze niet lijken op te wegen tegen het nadeel dat steeds grotere hoeveelheid (persoons)gegevens verwerkt kunnen worden. De ene vindt dat we eerst moeten afwachten of de markt zelf met afdoende en werkbare oplossingen komt, de andere vindt dat het geen kwaad kan om nu reeds proberen te te vatten welke problemen bij een grootschalige toepassing van RFID kunnen rijzen en deze proberen te voorkomen.

De Europese Commissie wijst er op dat echter ook het omgekeerde waar is. RFID is op technologisch en commercieel gebied klaar om massaal ingezet te worden in de maatschappij, maar o.a. het ontbreken van een duidelijk wetgevend en/of zelfregulerend kader en dus het ontbreken van rechtszekerheid, laat potentiële gebruikers toch nog afwachten[82]. Daarenboven zullen de voordelen van RFID nooit gerealiseerd worden indien de toepassing van RFID niet zowel op sociaal, politiek als ethisch vlak geaccepteerd wordt[83]. Bits of Freedom vraagt, in tegenstelling tot de bedrijfswereld, wel naar een aantal concrete aanvullingen van de wetgeving. Ten eerste wil ze een wettelijk verplichte controle over de beveiliging van alle RFID-toepassingen door onafhankelijke derden instellen. De resultaten van die controle moeten ten tweede gepubliceerd worden en ten derde dringen zij ook aan op het invoeren van een klachtenregeling waarbij misbruiken van de nieuwe technologieën, zowel door de bedrijfswereld als door de overheid, bestraft kan worden[84].

Ten slotte is er nog één opmerking die meerdere keren terug komt in de literatuur en dat is dat er te weinig nagedacht wordt over het behoud van anonimiteit bij de het gebruik van RFID. Zelfs het ECP.NL dringt er op aan

---

[80] W. SCHREURS, "Privacy en RFID-technologie", *P&I*, 2005, nr. 5, 200-201.

[81] Legal IST Project, *Report on additional legal issues*, 2006, http://www.ve-forum.org/projects/P1507/D15%20Report%20on%20Additional%20Legal%20Issues%20-%20final%20version.pdf, laatst geconsulteerd op 5 mei 2007, 6; B. SCHERMER, "Big Brother in een kleine Chip?", *JAVI* (Ned.), 2004, nr. 5, 162-163; J. VAN SCHOONHOVEN, "Scheiding der machten bij of krachtens de WBP", *P&I*, 2006, afl. 5, 216 en 220.

[82] Communication from the commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, *Radio Frequency Identification (RFID) in Europe: steps towards a policy framework*, 2007, http://ec.europa.eu/information_society/policy/rfid/doc/rfid_en.pdf, laatst geconsulteerd op 7 mei 2007, 4.

[83] Communication from the commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, *o.c.*, 5.

[84] S. NAS, "Iedereen een chippie in zijn arm? RFID-labels en de wolk van gegevens", *P&I*, 2005, nr. 3, 108.

om zo veel als mogelijk gebruik te maken van anonieme gegevens. Bedrijven bewijzen zichzelf hiermee trouwens een grote dienst. Zo moeten zij zich dan immers geen zorgen maken over de waarborgen van gegevensbeschermingswetgeving. Daarenboven zal het gebruik van RFID wanneer ze niet gekoppeld wordt aan identificerende gegevens gemakkelijker door de publieke opinie aanvaard worden[85].

4.2. EIGEN MENING

Ook ik ben de mening toegedaan dat we zeker geen paniekwetgeving mogen opstellen. Wij hebben in Europa en in België een aanzienlijke bescherming tegen onrechtmatig gebruik of onrechtmatige verwerking van persoonsgegevens die waarschijnlijk volstaat, ook voor nieuwe technologieën *an sich*. Toch maak ook ik mij zorgen over de hoeveelheid aan gegevens die zeer gemakkelijk en zeer snel verzameld, maar ook en vooral aan elkaar gelinkt kan worden. Of (nieuwe) wetgeving cumulatie van gegevens ooit zal kunnen verhinderen durf ik echter te betwijfelen.

Ten eerste ben ik geen voorstander van doorgedreven regulering. Indien men voor RFID per sector regeltjes gaat opleggen creëert men niet alleen een sectorspecifieke, maar ook technologiespecifieke wetgeving. Hoewel consumentenorganisaties niets liever zouden hebben, ben ik daar om twee redenen tegen gekant. Dit gaat ten eerste in tegen elke tendens tot techniekonafhankelijke wetgeving en ten tweede creëert dit hoogstwaarschijnlijk evenveel rechtsonzekerheid als het laten van een blinde vlek. Daarenboven wil ik er op wijzen dat we het feit dat we de vandaag bestaande wetgeving ook kunnen toepassen op RFID volledig te danken hebben aan de techniek onafhankelijke formulering van die wetgevingen.

Ten tweede denk ik dat ECP.NL toch iets te gemakkelijk kiest voor zelfregulering. Bedrijven mogen dan wel beseffen dat ze de consumenten achter zich moeten krijgen om niet geboycot te worden, er zullen steeds megagiganten blijven bestaan die ook zonder de steun van de consument kunnen omdat ze groot genoeg zijn of omdat er geen volwaardig alternatief bestaat.

Op het vlak van de praktische invulling van de wetgeving deel ik de mening van het ECP.NL wel. De consument moet op dit moment vooral goed geïnformeerd worden. Daarom zijn verplichte symbolen op de verpakkingen alvast een goed idee. Wat ik echter het aller belangrijkste vind, en daarin deel in de mening van Wim Schreurs, is dat de keuzevrijheid van iedere persoon te allen tijde gerespecteerd blijft. Daartoe kan een symbool op de verpakking al helpen, maar dan moeten er natuurlijk ook producten zonder RFID blijven bestaan. Omdat het onwaarschijnlijk is dat dezelfde producten met én zonder RFID technologie geproduceerd zullen worden, lijkt mij op dit moment een opt-in verplichting de enige oplossing, althans toch voor deze situaties waarin

[85] S. NAS, *o.c.*, 108-109

de toestemming van de persoon de enige rechtsgrond is tot verzameling van gegevens. Dit recht op een ongedwongen keuze zou daarenboven veel geholpen kunnen worden door de erkenning van een "recht op anonimiteit" in Europa. Hierop kom ik hieronder nog terug.

5. RECHTSVERGELIJKEND

5.1. RECHTSVERGELIJKING MET NEDERLAND

Aangezien ook Nederland moet voldoen aan de Data Protection Richtlijn van 1995, zal de invulling van nationale privacy bescherming gelijklopend zijn met die van België. Toch zien we dat in Nederland de problematiek rond nieuwe technologieën en eventuele nieuwe privacyschendingen veel meer aandacht krijgt. Dat heeft hoogstwaarschijnlijk te maken met het feit dat Nederland één van de koplopers is bij de ontwikkeling en productie van RFID.

Zowel België als Nederland benadrukken dat de discussie rond privacyvraagstukken niet in absolute termen gevoerd mag worden, maar dat het moet gaan om wie welke gegevens in welke gevallen en voor welk gebruik mag aanwenden.

In België wordt benadrukt dat de veiligheid, integriteit en vertrouwelijkheid van informatie gewaarborgd moet worden a.h.v. een geïntegreerd geheel van structurele, organisatorische, technische, fysische en andere veiligheidsmaatregelen. Bij de invoering van de nieuwe elektronische identiteitskaart bijvoorbeeld werd daarom een onafhankelijk comité opgericht dat elke elektronische uitwisseling van persoonsgegevens preventief toetst op de conformiteit met de geldende toezichtsmechanismen[86]. Hetzelfde zou kunnen ingevoerd worden bij het gebruik van RFID.

In Nederland lijkt men voor preventieve toezichtsmechanismen minder open te staan. Door meerdere auteurs wordt benadrukt dat er geen paniekwetgeving mag gecreëerd worden en dat zelfregulering een kans moet krijgen. In deze zin leunen zij ook dichter aan bij het Amerikaanse uitgangspunt[87].

5.2. RECHTSVERGELIJKEND MET DE VS

Er bestaan tussen Amerika en Europa drie grote verschillen. Ten eerste kent men in Amerika geen uitdrukkelijke bescherming van "de privacy". Ten tweede kent men in Amerika wel een uitdrukkelijke erkenning van het recht op anonimiteit, wat men in Europa dan weer niet kent. Ten slotte is de Europese regelgeving zowel van toepassing op private als publieke organen, maar in Amerika is dat veelal niet het geval.

---

[86] D. DE BOT, *Privacybescherming bij e-government in België*, in *CPR Collectie Publiekrecht*, Brugge, Vanden Broele, 2005, 14-21.
[87] D. DE BOT, *o.c.*, 15-16; W. SCHREURS, *o.c.*, 200-201; B. SCHERMER, *o.c.*, 160-162.

Een algemeen recht op privacy bestaat er in Amerika niet. Dat wil echter niet zeggen dat de privacy er niet beschermd wordt. Historisch gezien zijn zelfs de eerste publicaties over "recht op een privé-leven", waaronder het baanbrekende werk van Brandeis en Warren, van Amerikaanse hand[88]. Ook de Fair Information Practice Principles zijn van Amerikaanse oorsprong. Het privacybegrip is er geëvolueerd van een *right to be left alone* naar een recht op individuele vrijheid en onafhankelijkheid gebaseerd op de algemene bescherming van de menselijke waardigheid en persoonlijkheid[89]. Toch zien we ook in het post 9/11 tijdperk dat het Amerikaanse privacybegrip nog sterk verschilt van het Europese. Langs de ene kant zien we dat er een hogere tolerantie is tegenover inbreuken op of beperking van het recht op privacy, met name wanneer het recht op privacy in conflict komt met '*security*'. Langs de andere kant laten de consumenten- en privacyrechtenorganisaties een veel luidere stem horen omdat regelgeving ter bescherming van de privacy, als ze er dan al is, voornamelijk waarborgen biedt tegen inmenging door de overheid en veel minder tegen inmengingen door bedrijven.

Het is namelijk zo dat de Amerikaanse Grondwet op geen enkele plaats privacy als begrip noch als recht vernoemt. Verspreid over de verschillende amendementen worden wel afzonderlijke rechten gewaarborgd zoals het recht om anoniem te spreken, de vrijheid van vereniging, verbod om tegen zichzelf te getuigen, het recht op bescherming tegen onredelijke huiszoekingen etc. Daaruit wordt ook het recht op anonimiteit afgeleid. Daarnaast wordt sinds het arrest *Katz. v. United States* door het Supreme Court ook erkend dat deze verschillende rechten moeten leiden tot *a protection of people, not places* en dat iedereen recht heeft op respect voor zijn privacy binnen de (Amerikaanse) *reasonable expectations of privacy*-leer[90].

De federale grondwet wordt aangevuld door de Grondwetten van de verschillende Staten. Sommige staten, zoals Alaska, California en Florida, hebben wel expliciet het recht op privacy opgenomen, maar ook deze bevatten dan weer enkel waarborgen tegen inmenging door de overheid en niet tegen inmenging door bedrijven. Ook zijn enkele deelstaten bezig met de ontwikkeling van een regeling voor het gebruik van RFID in scholen en door de regering, maar deze zijn nog nergens concreet[91].

Hetzelfde probleem stelt zich bij de Privacy Act van 1994 die een eerste poging vormde om de Fair Information Practice Principles afdwingbaar te maken. De private sector werd hier buiten gehouden, niet omdat zij niet geacht werden te moeten voldoen aan de beginselen van behoorlijk gegevensbeheer, maar omdat niet, of niet voldoende, was aangetoond dat de privé-sector de

[88] SOLVE, ROTENBERG en SCHWARTZ, *Information Privacy Law*, , Aspen publishers, 2006, 9-11.
[89] SOLVE, ROTENBERG en SCHWARTZ, *o.c.*, 33-35.
[90] Katz v. United States, 389 U.S. 347, 1967.
[91] Legal IST Project, *Report on additional legal issues*, 2006, http://www.ve-forum.org/projects/P1507/D15%20Report%20on%20Additional%20Legal%20Issues%20-%20final%20version.pdf, laatst geconsulteerd op 5 mei 2007, 55; Zie ook ECP.NL, *Privacyrechtelijke aspecten van RFID*, Efficiënta Offsetdrukkerij BV, 2005, 53-54.

privacybeginselen schonden[92].

Juist dat laatste idee is kenmerkend voor het hele Amerikaanse wetgevingssysteem: zij zijn in het algemeen zeer terughoudend t.a.v. regulering van de private sector. Dat is zeker het geval wanneer de vrijheid op informatie dreigt gecompromitteerd te worden of innovatie belemmerd dreigt te worden. Alleen wanneer het aantoonbaar uit de hand loopt acht men een ingrijpen door de overheid gerechtvaardigd. Indien de privé sector aangeeft vrijwillig (zelf opgestelde) gedragsregels te willen opvolgen, is overheidsregulering bijgevolg niet gerechtvaardigd. Zo gaat men er in de VS van uit dat *market imperfections must be compared with the imperfections of government regulations*. Zelfregulering, of het vrijwillig respecteren van de privacy, is ook in het geval van RFID dus de Amerikaanse boodschap.

6. VOORGESTELDE WETSWIJZIGINGEN

Zoals ik hierboven reeds duidelijk maakte ben ik geen voorstander van bijkomende reguleringen. Ten eerste creëert een kluwen van reguleringen enkel rechtsonzekerheid. Ten tweede zal RFID gerichte wetgeving toch steeds achter de feiten aan lopen. Het wetgevingsproces is nu eenmaal traag, zeker wanneer er verschillende belangen in conflict staan met elkaar en in het geval van RFID is dat het belang van de economie tegenover de algemene behaaglijkheid van iedere burger. Ten derde denk ik dat het probleem niet schuilt in de RFID technologie zelf, maar in de door eenvoudige koppeling van databasen enorme cumulatie van informatie. Zoals hierboven ook aangeduid maakt RFID het weliswaar veel eenvoudiger om gegevens te verzamelen, maar blijven de verzamelde gegevens in vele toepassingen van beperkt nut zodat het principe van doelgebonden verzameling niet in gevaar is. Dat principe wordt echter wel bedreigd door de verbinding van de databanken achter de RFID technologie.

Het is bijgevolg niet nodig om het gebruik van RFID op zich te limiteren, maar om te voorkomen dat het bezit en de cumulatie van databanken macht creëert. Daarom pleit ik voor anonimiteit. Daar waar het kan, moet de anonieme verzameling van gegevens verplicht worden. Daar waar dat niet kan, moet iedere individuele persoon een keuzerecht krijgen. We moeten aan de bron optreden om een ongecontroleerde informatiestroom te kunnen voorkomen.

Een eerste aanzet tot een recht op anonimiteit werd gegeven in de Richtlijn Elektronische communicatie. Daarin wordt de ontwikkeling van een anonieme toegang tot publieke netwerken als internet en telefonie aangemoedigd. Er wordt ook gewezen op de noodzaak om de verwerking van persoonsgegevens te minimaliseren en waar mogelijk gebruik te maken van geanonimiseerde of gepseudonimiseerde gegevens. Zoals hierboven reeds vermeld is het echter

[92] P. CAREY, *E-privacy and online data protection*, Londen, Butterworths LexisNexis, 2002, 29-31; SOLVE, ROTENBERG en SCHWARTZ, *Information Privacy Law*, Aspen publishers, 2006, 579-581.

onduidelijk of deze richtlijn ook op RFID-technologie van toepassing is. Daarenboven werden deze overwegingen niet vertaald in bindende wetgeving. Om echter te vermijden dat het gebruik van RFID niet in een rechtsvacuüm terecht komt, stel ik wel voor een aantal praktische regelingen uit te werken die voornamelijk tot doel moeten hebben de consument te informeren. Ten eerste moet de afbeelding van een universeel RFID-symbool op de verpakking van producten die RFID bevatten verplicht worden. Ten tweede moet ook aan gebouwen waarin men gebruik maakt van RFID dit symbool duidelijk zichtbaar aangebracht worden. Ten derde moet voorkomen worden dat de keuzevrijheid beperkt of gemanipuleerd wordt. Daartoe moet een recht op anonimiteit erkend worden en moet er in consumentenzaken een verbod komen aan het geven van extra voordelen in ruil voor toestemming tot verwerking van persoonsgegevens d.m.v. RFID. Daartoe moet er ten slotte ook, althans voorlopig, een *opt-in* recht erkend worden voor elke verwerking van persoonsgegevens d.m.v. RFID die als enige rechtsgrond de toestemming van de persoon heeft. Wanneer de technologie daartoe op punt staat, kan deze *opt-in* verplichting vervangen worden door een *opt-out* mogelijkheid.

7. BESLUIT

Niet elke toepassing van RFID-technologie vormt een bedreiging voor onze privacy, maar indien er onzorgvuldig of onrechtmatig gebruik van gemaakt wordt, komt voornamelijk ons recht op informationele zelfbeschikking toch onder druk te staan. Deze druk stijgt naarmate ook de, eventueel zelfs heimelijk, verzamelde hoeveelheid persoonsgegevens stijgt. Onze privacy wordt beschermd door techniekonafhankelijk geformuleerde grondrechten en mensenrechten en door de op Europees niveau voorziene bescherming van persoonsgegevens. Over de vraag of de bestaande wetgeving genoeg bescherming biedt, bestaat discussie. Deze discussie wordt sterk gekleurd door de verschillende belangen die een rol spelen. Met name staan de economische belangen haaks op de algemene behaaglijkheid van ieder individu. Toch denk ik dat we zeker geen paniekwetgeving mogen creëren, maar d.m.v. een aantal eenvoudige oplossingen zoals de verplichte vermelding van het gebruik van RFID, een goede informering van de consument en een groot respect voor de keuzevrijheid van ieder individu, een vlotte opname van toch wel zeer vooruitstrevende technologie in onze maatschappij kunnen verzekeren.