Advies van het Europees Economisch en Sociaal Comité over Radiofrequentie-identificatie (RFID)

(2007/C 256/13)

De Europese Commissie heeft het Europees Economisch en Sociaal Comité op 26 februari 2007, overeenkomstig artikel 262 van het Verdrag tot oprichting van de Europese Gemeenschap, per brief verzocht een advies op te stellen over *Radiofrequentie-identificatie (RFID)*.

De gespecialiseerde afdeling Vervoer, energie, infrastructuur en informatiemaatschappij, die met de voorbereidende werkzaamheden was belast, heeft haar advies op 19 juni 2007 goedgekeurd. Rapporteur was de heer Morgan.

Tijdens zijn 437e zitting van 11 en 12 juli 2007 (vergadering van 11 juli) heeft het Europees Economisch en Sociaal Comité met 138 stemmen voor en 1 stem tegen, bij 6 onthoudingen, het volgende advies uitgebracht:

1. **Conclusies en aanbevelingen**

1.1 Radiofrequentie-identificatie (RFID) is een waardevolle technologie, die op termijn van groot belang zal worden. De huidige en toekomstige toepassingen van RFID kunnen tal van bedrijfsprocessen in zowel de publieke als de private sector verbeteren en kunnen voor zowel natuurlijke personen als ondernemingen aanzienlijke voordelen opleveren. RFID kan tevens tot een enorme ontwikkeling van internettoepassingen leiden, zodat uiteindelijk iets ontstaat wat door een VN-agentschap is omschreven als het „internet van dingen". Maar RFID kan ook, als het niet uiterst nauwgezet wordt gecontroleerd, de privacy van mensen schenden, de burgerlijke vrijheden ondermijnen en de veiligheid van personen en ondernemingen in gevaar brengen.

1.2 De volledige titel van deze mededeling luidt: „Radiofrequentie-identificatie (RFID) in Europa: maatregelen met het oog op een beleidskader". Voorafgaand aan deze mededeling heeft de Commissie al een brede raadpleging gehouden. Het EESC wordt nu verzocht een verkennend advies op te stellen. Op grond van de reacties op de mededeling zal de Commissie tegen het eind van het jaar een aanbeveling aan de lidstaten doen. Eventuele wetgeving, die meer tijd vergt, volgt later. In dit advies moet het Comité zich dus concentreren op de inhoud van die aanbeveling.

1.3 De Commissie heeft besloten een groep van belanghebbenden op te richten, die haar moet helpen met de formulering van aanbevelingen en als klankbord moet dienen. Het Comité zou zijn advies graag aan de groep van belanghebbenden willen voorleggen.

1.4 Het Comité steunt de door de Commissie voorgestelde maatregelen op het gebied van radiospectrum, normen, gezondheid, veiligheid en milieu en vindt dat de EU absoluut een wezenlijke industriële bijdrage moet leveren aan het overleg over normalisatie.

1.5 Aangezien de Commissie haar aanbevelingen aan de lidstaten eind dit jaar zal publiceren, mag redelijkerwijs worden aangenomen dat zij de *status quo* op het gebied van gegevensbeveiliging en privacy zal handhaven. Concreet betekent dit dat de bestaande nationale instanties die over gegevensbescherming waken, ook verantwoordelijk zullen worden voor alles wat op het vlak van RFID met privacy en gegevensbescherming heeft te maken. Daarover gaat dit advies.

1.6 De privacy en burgerlijke vrijheden worden ernstig bedreigd door RFID want:

— RFID-tags kunnen worden aangebracht in/op voorwerpen en documenten zonder dat de ontvanger hier iets van merkt. Omdat radiogolven gemakkelijk en geluidloos door stof, plastic en ander materiaal heen gaan, kunnen RFID-tags die in kleding zijn genaaid of op voorwerpen zijn aangebracht die in handtassen, winkeltassen, koffers e.d. worden vervoerd, worden gelezen;

— met een elektronische productcode kan elk voorwerp op aarde van een eigen, unieke ID worden voorzien. Het gebruik van unieke ID-nummers kan leiden tot een wereldwijd registratiesysteem waarbij elk voorwerp wordt geïdentificeerd en op het moment van verkoop of overdracht aan zijn koper of eigenaar wordt gekoppeld;

— het gebruik van RFID vergt het opzetten van grote databanken met unieke tag-gegevens. Deze bestanden kunnen worden gekoppeld aan persoonlijke identificatiegegevens, vooral naarmate de geheugens en de verwerkingscapaciteit van computers zich uitbreiden;

— tags kunnen vanaf een afstand worden gelezen, ook buiten het gezichtsveld, door lezers (scanners) die onzichtbaar kunnen worden verwerkt in bijna elke omgeving waar mensen samenkomen. Lezers kunnen worden aangebracht in vloertegels, verwerkt in tapijt, verborgen in deuropeningen en verstopt in kasten, waardoor het voor iemand vrijwel onmogelijk wordt om erachter te komen wanneer hij of zij wordt gescand;

— indien persoonlijke identiteit wordt gekoppeld aan unieke RFID-tagnummers, kunnen mensen zonder dat zij het weten of zonder dat zij hiervoor toestemming hebben verleend worden opgespoord of geprofileerd;

— een wereld waarin RFID-lezers een allesomvattend, wereldwijd netwerk vormen is niet ondenkbaar. Voor een dergelijk netwerk zijn niet overal lezers nodig. In Londen worden alle auto's die het centrum van Londen binnenkomen voor de congestieheffing met relatief weinig, strategisch geplaatste camera's gefotografeerd. Een netwerk van strategisch geplaatste RFID-lezers kan op dezelfde manier worden opgezet. Dat mag niet gebeuren.

1.7 De consequenties van deze bedreigingen zijn:

— RFID-gebruikers moeten hun beleid en praktijken openbaar maken en er mogen geen geheime databanken betreffende persoonsgegevens zijn.

— Iedereen heeft het recht te weten of producten in winkels RFID-tags of -lezers bevatten. Indien er in winkels sprake is van het lezen van tags, moet dit op een voor alle partijen transparante wijze gebeuren.

— RFID-gebruikers moeten bekendmaken voor welke doeleinden tags en lezers worden gebruikt. Alleen de informatie die noodzakelijk is voor het beoogde doel, mag worden verzameld.

— RFID-gebruikers zijn verantwoordelijk voor de toepassing van de technologie en moeten erop toezien dat e.e.a. binnen de grenzen van de wetgeving en richtlijnen inzake gegevensbeveiliging gebeurt. Zij zijn ook verantwoordelijk voor de veiligheid en volledigheid van het systeem en zijn databank.

1.8 Hoe deze principes in de praktijk moeten worden gebracht, is nog niet duidelijk. In het gunstigste geval geven alle bedrijven die met de consument zaken doen, zoals winkeliers, kaartverkopers, toegangscontroleurs of vervoerders hun klanten een soort garantie dat deze principes in acht zullen worden genomen, een soort klantenhandvest. Een dergelijk handvest zou alle beginselen van goede praktijken m.b.t. gegevensbescherming zoals omschreven in par. 4.5 kunnen bevatten. Daarnaast stelt het Comité de volgende richtsnoeren voor:

a) Handelaren mogen hun klanten niet verplichten te accepteren dat de producten die zij kopen actieve of passieve tags bevatten. Als alternatief kunnen de tags op de verpakking worden aangebracht of kan gebruik gemaakt worden van verwijderbare tags (zoals bij prijskaartjes).

b) Klanten moeten de tags op de voorwerpen die zij in hun bezit hebben kunnen verwijderen of de-activeren.

c) RFID mag in principe niet worden gebruikt om personen te volgen. Het opsporen van mensen is onaanvaardbaar, of dat nu bijvoorbeeld via kleding, goederen, kaarten of andere dingen gebeurt.

d) RFID mag nooit worden gebruikt op een manier die de anonimiteit kan opheffen of beperken.

e) De verantwoordelijke instantie zou duidelijk moeten maken dat c) en d) alleen zijn toegestaan in uitzonderlijke omstandigheden en met voorafgaande, formele kennisgeving aan de instantie.

1.9 Op het bovenstaande kunnen bepaalde uitzonderingen worden toegestaan wanneer

— natuurlijke personen ervoor kiezen om de tags te behouden voor persoonlijke doeleinden;

— natuurlijke personen ermee instemmen dat hun gangen kunnen worden nagegaan wanneer zij zich in een kritische omgeving bevinden, zoals streng beveiligde openbare en private gebouwen en instellingen;

— natuurlijke personen ervoor kiezen om toepassingen te gebruiken waarmee zij, net als door het gebruik van mobiele telefoons, pinpassen, internetadressen enz., kunnen worden gelokaliseerd en geïdentificeerd.

De verantwoordelijke instantie moet van dergelijke uitzonderingen op de hoogte worden gebracht.

1.10 RFID is nog niet uitontwikkeld, dus nog niet alle mogelijkheden zijn bekend. Enerzijds kan RFID van onschatbare waarde zijn voor onze technologische beschaving, maar anderzijds kan het de grootste bedreiging ooit voor privacy en vrijheid zijn. Het Comité is van mening dat de ontwikkeling van RFID-toepassingen moet doorgaan, maar dat zulks volgens strikte ethische regels en zonder aantasting van privacy, vrijheid en gegevensbescherming moet gebeuren.

1.11 Kortom, waar RFID-toepassingen worden toegestaan, moet het gebruik ervan volkomen transparant zijn voor alle betrokkenen. Toepassingen die de behandeling van goederen verbeteren, zijn algemeen aanvaardbaar. Toepassingen waarbij mensen van tags worden voorzien, zijn in het algemeen onaanvaardbaar, behalve in tijdelijke situaties. Toepassingen die mensen en goederen met elkaar verbinden, kunnen aanvaardbaar zijn voor marketingdoeleinden. Toepassingen waarbij mensen worden geïdentificeerd aan de hand van de goederen die zij hebben gekocht, zijn over het algemeen onaanvaardbaar. Sommige toepassingen zijn sowieso onaanvaardbaar in een vrije maatschappij en mogen nooit worden toegestaan. De dwingende noodzaak om privacy en anonimiteit in stand te houden moet de kern van de aanbeveling van de Commissie aan de lidstaten zijn.

2. **Wat is RFID en wat is het belang ervan?**

2.1 Radiofrequentie-identificatie (RFID) is een technologie met behulp waarvan gegevens via radiofrequenties automatisch geïdentificeerd en gelezen kunnen worden. Het opmerkelijke aan deze technologie is dat een unieke identificatiecode en andere informatie — met behulp van een microchip — aan om het even welk voorwerp, welk dier of zelfs welke persoon kunnen worden vastgemaakt, waarna deze informatie draadloos kan worden gelezen.

2.2 De tags zelf bestaan uit een elektronisch circuit dat gegevens opslaat, en een antenne die de gegevens via radiogolven doorgeeft. De opgeslagen informatie wordt door een RFID-lezer opgevangen. Wanneer de lezer radiogolven uitzendt, legt hij contact met alle tags binnen zijn bereik. Met behulp van software wordt de lezer gestuurd en wordt de informatie verzameld en gefilterd.

2.3 Er zijn verschillende soorten RFID-systemen. Tags zijn ofwel actief ofwel passief. Actieve tags bevatten een batterij die het interne circuit aanstuurt en radiogolven opwekt, die ook zonder RFID-lezer kunnen worden uitgezonden. Passieve tags hebben geen eigen energiebron en worden aangedreven door de energie van de radiogolf die wordt uitgezonden door de lezer. Tags zijn „alleen lezen" of „lezen-schrijven". „Alleen lezen-tags" zijn goedkoper en worden in de meeste huidige toepassingen gebruikt.

2.4 Het bereik van een RFID-systeem hangt af van de radiofrequentie, het vermogen van de lezer en het materiaal tussen de tag en de lezer. Het bereik kan variëren van een paar meter voor passieve systemen tot meer dan 100 meter voor actieve systemen.

2.5 RFID staat onderaan in de hiërarchie van draadloze technologie. Naar gelang van de afstand die de signalen moeten afleggen is de rangorde als volgt: bovenaan staan satellietcommunicatiesystemen zoals GPS. Dan komt mobiele breedbandtechnologie als GSM en GPRS, gevolgd door signalen met een korter bereik binnen gebouwen zoals Wi Fi, persoonlijke netwerken zoals Bluetooth, en tot slot RFID. Elk van deze technologieën staat op zichzelf en is onafhankelijk, zodat er bijvoorbeeld geen risico bestaat dat satellietsystemen de RFID-tags lezen. Niettemin kunnen gegevens worden uitgewisseld tussen de diverse systemen door apparaten als mobiele telefoons.

2.6 Hieronder volgt een aantal voorbeelden van mogelijke voordelen van RFID-toepassingen:

— voor een natuurlijke persoon kan RFID veiligheid betekenen (bijv. voedselveiligheid, gezondheidszorg, bestrijding van vervalsing), gemak (kortere rijen bij de kassa, betere bagagebehandeling in luchthavens, automatische betalingen) en betere patiëntenzorg, vooral in geval van chronische ziekten zoals dementie;

— in het vervoer kan RFID de doeltreffendheid, veiligheid en servicekwaliteit voor personen en goederen verbeteren;

— in de gezondheidszorg kan RFID de kwaliteit van de zorg en de veiligheid van de patiënt verbeteren, en kan het bijdragen tot een betere naleving van het medicatieschema en een betere logistiek; aan RFID-tags op pillen wordt nog gewerkt;

— in de detailhandel zou met behulp van RFID productschaarste kunnen worden voorkomen, het voorraadpeil kunnen worden bijgehouden en diefstal kunnen worden bestreden;

— in bedrijven die met productvervalsing hebben te maken, kan met behulp van RFID worden nagegaan waar illegale goederen de productieketen binnenkomen;

— verwacht wordt dat met RFID-tags het sorteren en recycleren van productonderdelen en materialen zal verbeteren, hetgeen positieve gevolgen zal hebben voor afvalbeheer en duurzame ontwikkeling.

2.7 Ter illustratie van de vele aspecten van RFID volgt hier een voorbeeld van de toepassing op boeken. De hoeveelheid boeken in druk is op zich al een logistieke nachtmerrie voor uitgevers, distributeurs, bibliotheken en handelaren. Zodra het logistieke gedeelte achter de rug is en een boek eenmaal de plank heeft bereikt, moet worden bijgehouden waar het boek zich bevindt, zodat het kan worden teruggevonden en vervangen. Daarnaast moeten bibliotheken zicht houden op hun uitleenbestand, terwijl de lezer die liever zijn boeken koopt, soms moeite heeft met het bijhouden van wat hij in de kast heeft staan. RFID-tags op boeken bieden een oplossing voor al deze problemen. Wat voor de uitgeleende boeken van bibliotheken geldt, geldt ook voor andere situaties waarin voorwerpen in omloop zijn of worden verhuurd.

2.8 Om te illustreren welke gevaren aan deze technologie kleven, is hieronder een passage opgenomen uit een octrooiaanvraag van IBM (20020615758) van november 2002. Het gaat over het identificeren en traceren van personen die gebruik maken van voorwerpen met een RFID-tag.

> *„Een methode en systeem voor het identificeren en traceren van personen die voorwerpen met een RFID-tag dragen. De aankoopgegevens van iedereen die iets in een winkel koopt worden verzameld door terminals op verkooppunten en opgeslagen in een transactiebestand. Wanneer een persoon die een voorwerp met een RFID-tag bij zich draagt of aanheeft, de winkel of een ander gemarkeerd gebied binnengaat, worden de RFID-tags op die persoon gescand door een daar aanwezige scanner en wordt de informatie op de tags gelezen. De informatie van de RFID-tag wordt gekoppeld aan de transactiegegevens die in het transactiebestand zijn opgeslagen volgens bekende correlatiealgoritmen. Aan de hand van de resultaten van deze koppeling kan de exacte identiteit van de persoon of kunnen bepaalde kenmerken van die persoon worden vastgesteld. Deze informatie wordt gebruikt om de bewegingen van de persoon door de winkel of op andere plaatsen te volgen".*

Octrooiaanvraag 20050038718 van American Express luidt ongeveer hetzelfde.

2.9 RFID is duidelijk veel meer dan een streepjescode. Uit de hierboven aangehaalde octrooiaanvraag blijken de belangrijkste verschillen:

a) een tag bevat niet alleen een beschrijving van het voorwerp maar ook een unieke identificatiecode die, op zijn beurt, de koper kan identificeren;

b) een tag hoeft geen microchip te zijn; de circuits kunnen rechtstreeks op de meeste materialen, zoals stof, worden geprint;

c) een tag kan ook na verkoop blijven bestaan en kan aldus voortdurend opnieuw worden gelezen;

d) taglezers bevinden zich niet alleen op verkooppunten maar kunnen overal staan, niet alleen op het terrein van de winkelier;

e) koppeling aan een databank geeft een nieuwe dimensie aan gegevensverzameling, privacy en gegevensbeveiliging.

2.10 Of een tag ook buiten het winkelcircuit mag worden gebruikt, is een punt van discussie. Enerzijds vormt het een bedreiging van de privacy. Anderzijds kan de consument erbij gebaat zijn. Met behulp van RFID-lezers thuis kan bijvoorbeeld de organisatie van wijnkelders, koelkasten, garderobes en bibliotheken een stuk eenvoudiger worden. Het spreekt voor zich dat iedereen hierin de vrije keuze moet hebben, maar de technologie en de toepassing moeten die keuze wél mogelijk maken.

2.11 RFID wordt voor veel meer doeleinden dan alleen productidentificatie gebruikt. Uw EESC-dienstpas is voorzien van een RFID-tag. In de Londense metro worden op grote schaal RFID-kaarten gebruikt voor betaling en toegang. Binnenkort worden ook kredietkaarten uitgerust met een RFID-tag voor de betaling van kleine bedragen zonder pincode. De technologie wordt ook gebruikt voor tolheffing en de identificatie van chauffeurs. In sommige Europese ski-oorden krijg je toegang tot de skilift met een RFID-plaatje in de zak van je skipak. Uw rapporteur loopt dagelijks rond met drie RFID-kaarten en één RFID-plaatje. Zijn hond heeft onderhuids een RFID-chip ingeplant gekregen. Dit soort chips wordt binnenkort wereldwijd gebruikt voor het merken en traceren van dieren in de voedselketen. En dan is het maar een kleine stap naar het merken van misdadigers en probleempatiënten, net als honden.

2.12 Het gebruik van RFID-technologie in identiteitskaarten zoals de dienstpas van het EESC is een onschuldige toepassing. Maar het wordt allemaal wat minder onschuldig wanneer RFID-tags in werkkleding of uniformen worden aangebracht, zodat de handel en wandel van werknemers constant kan worden gevolgd door scanners die overal op de werkvloer staan opgesteld. Daarbij moet wel worden opgemerkt dat zulks om bijv. veiligheidsredenen in sommige gevallen wenselijk kan zijn. Hoe dan ook, zonder adequate waarborgen nagaan waar iemand zich bevindt zou een grove schending van de privacy opleveren en zou daarom uitsluitend om gegronde redenen en onder nauwkeurig toezicht mogelijk moeten zijn.

2.13 Als voorbode van bizarre toepassingen noemt *The Economist* het toegangskaartje voor de VIP-area van de Baja Beach Club in Barcelona: een microchip die in de arm van de klant wordt geplant. Met behulp van deze chip, die amper groter is dan een rijstkorrel omhuld door glas en siliconen, worden mensen geïdentificeerd bij binnenkomst en bij het bestellen van een drankje. De chip wordt onder plaatselijke verdoving door een verpleegster geïnjecteerd. In wezen gaat het hier ook om een RFID-tag.

3. **Inhoud van de mededeling**

3.1 RFID is beleidsmatig van groot belang omdat zij een stuwende kracht kan betekenen voor groei en werkgelegenheid en zo een belangrijke bijdrage kan leveren aan de Lissabonstrategie, op voorwaarde dat de obstakels voor innovatie uit de weg kunnen worden geruimd.

3.2 Met het oog hierop heeft de Commissie in 2006 een openbare raadpleging georganiseerd over RFID, waarin duidelijk werd welke verwachtingen men kan koesteren op basis van de resultaten van de RFID-pioniers maar ook welke bezorgdheid er leeft bij de burgers over RFID-toepassingen wanneer het gaat om het identificeren en/of volgen van personen.

3.3 Verdere ontwikkeling en een bredere invoering van RFID-technologie zouden de rol van informatie- en communicatietechnologieën (ICT) nog moeten versterken door innovatie en economische groei te bevorderen.

3.4 Er is vooral behoefte aan een duidelijk en voorspelbaar rechts- en beleidskader om deze nieuwe technologie aanvaardbaar te maken voor gebruikers. Omdat RFID van nature grensoverschrijdend is, moet dit kader er eveneens voor zorgen dat de regelgeving in overeenstemming is met de interne markt.

3.5 *Veiligheid, privacy en ethiek*

3.5.1 Er bestaat grote vrees dat deze technologie, die nieuwe toepassingen mogelijk maakt en overal inzetbaar is, een bedreiging zou kunnen vormen voor de privacy: RFID-technologie zou gebruikt kunnen worden om informatie te verzamelen die al dan niet rechtstreeks wordt gekoppeld aan een identificeerbare of geïdentificeerde persoon zodat het om persoonsgegevens gaat; RFID-tags kunnen persoonsgegevens opslaan; RFID-technologie zou gebruikt kunnen worden om de bewegingen van personen te volgen of een gedragsprofiel op te stellen. RFID heeft het potentieel van een technologie die een inbreuk zou kunnen vormen op de persoonlijke levenssfeer. Er is bezorgdheid geuit over de mogelijke schending van fundamentele waarden en privacy en over meer toezicht, met name op het werk, hetgeen zou kunnen leiden tot discriminatie, uitsluiting, represailles en mogelijk verlies van baan.

3.5.2 Het is duidelijk dat de toepassing van RFID maatschappelijk en politiek aanvaardbaar, moreel toelaatbaar en wettelijk toegestaan moet zijn. RFID kan alleen tal van economische en maatschappelijke voordelen bieden wanneer doelmatige waarborgen worden gegeven voor de inachtneming van gegevensbescherming en privacy en de hiermee verbonden morele dimensies die ten grondslag liggen aan de discussie over de maatschappelijke aanvaarding van RFID.

3.5.3 Het communautaire rechtskader inzake gegevensbescherming en privacy in Europa was zodanig opgezet dat het bestand zou zijn tegen innovatie. De bescherming van persoonsgegevens valt onder de algemene richtlijn Gegevensbescherming ([1]), die van toepassing is op alle technologieën, met inbegrip van RFID. De algemene richtlijn Gegevensbescherming wordt aangevuld door de ePrivacy-richtlijn ([2]). Op grond van deze richtlijnen moeten de nationale autoriteiten van de lidstaten erop toezien dat de invoering van RFID-toepassingen in overeenstemming is met de wetgeving inzake privacy en gegevensbescherming. Het kan dan ook noodzakelijk zijn gedetailleerde richtsnoeren te formuleren over de praktische tenuitvoerlegging van RFID-toepassingen en specifieke gedragscodes op te stellen.

3.5.4 Op het gebied van de beveiliging moeten het bedrijfsleven, de lidstaten en de Commissie hun krachten bundelen om meer inzicht te krijgen in systeemvraagstukken en de hieraan verbonden veiligheidsrisico's die zich kunnen voordoen wanneer RFID-technologieën en systemen op grote schaal worden toegepast. Om dergelijke uitdagingen het hoofd te bieden moet met name aandacht worden besteed aan het formuleren en goedkeuren van de ontwerpcriteria die de risico's voor privacy en beveiliging beperken, niet alleen op technologisch maar ook op organisatorisch vlak en bij het bedrijfsproces. Een grondig onderzoek van de kosten en baten van specifieke risico's voor veiligheid en privacy voordat RFID-systemen worden geselecteerd en RFID-toepassingen worden ingevoerd, is dan ook noodzakelijk.

3.5.5 Er is bezorgdheid over de openheid en neutraliteit van de databanken die de unieke identificatiecodes zullen registeren welke ten grondslag liggen aan het RFID-systeem, de opslag en verwerking van de bijeengebrachte gegevens, met inbegrip van het gebruik ervan door derde partijen. Dit is een belangrijk vraagstuk met het oog op de rol van RFID als stuwende kracht voor een nieuwe ontwikkelingsfase van het internet waarbij uiteindelijk miljarden intelligente instrumenten en gesofistikeerde sensortechnologieën in een wereldwijde communicatienetwerkinfrastructuur met elkaar zullen zijn verbonden. Deze nieuwe fase in de ontwikkeling van het internet wordt ook wel het „internet van dingen" genoemd.

3.5.6 Het systeem voor de registratie en benaming van identiteiten in dit toekomstige „internet van dingen" moet waarborgen bieden tegen systeemuitval of onbevoegd gebruik, die desastreus zouden kunnen zijn. Het zou niet in handen mogen vallen van bijzondere belangengroeperingen die deze databanken en benoemingssystemen voor hun eigen doeleinden kunnen gebruiken. Voorts zou met betrekking tot de veiligheid, ethiek en privacybescherming rekening moeten worden gehouden met alle belanghebbenden, van natuurlijke personen tot ondernemingen, wier gevoelige bedrijfsinformatie is opgenomen in op RFID-gebaseerde bedrijfsprocessen.

3.5.7 Bij het ontwerp van het systeem zou rekening moeten worden gehouden met zowel de eisen van de actief bij de opbouw van het RFID-informatiesysteem betrokken partijen (bijvoorbeeld bedrijfsorganisaties, overheidsdiensten, ziekenhuizen) als die van de eindgebruikers die de doelgroep vormen (burgers, consumenten, patiënten, werknemers). Omdat eindgebruikers over het algemeen niet betrokken worden bij het ontwerp zal de Commissie steun verlenen aan de ontwikkeling van een reeks toepassingsgerichte richtsnoeren (gedragscode, goede praktijken) door een werkgroep van deskundigen die alle partijen vertegenwoordigen. Eind 2007 zal de Commissie een aanbeveling doen waarin de beginselen worden geformuleerd die overheidsdiensten en andere belanghebbenden moeten toepassen ten aanzien van het gebruik van RFID.

3.5.8 Voorts zal de Commissie nagaan welke bepalingen moeten worden opgenomen in het komende voorstel voor wijziging van de ePrivacy-richtlijn en tegelijkertijd rekening houden met de input van de toekomstige RFID-belangengroep, de groep Gegevensbescherming artikel 29 en andere relevante initiatieven zoals de Europese Adviesgroep inzake de ethiek van wetenschappen en nieuwe technologieën. Op deze basis zal de Commissie nagaan of verdere wetgevingsmaatregelen nodig zijn om de bescherming van gegevens en de persoonlijke levenssfeer te waarborgen.

3.5.9 De Commissie zal de ontwikkelingen in de richting van het „internet van dingen", waarvan RFID naar verwachting een belangrijk onderdeel zal vormen, op de voet blijven volgen. Eind 2008 zal de Commissie een mededeling publiceren waarin de aard en de gevolgen van deze ontwikkelingen zullen worden geanalyseerd, en waarin met name aandacht zal worden besteed aan privacy, vertrouwen en governance. Verder zal een evaluatie worden uitgevoerd van de beleidsopties en zal, om de bescherming van gegevens en privacy te waarborgen en andere beleidsdoelen te verwezenlijken, worden onderzocht of verdere wetgeving moet worden voorgesteld.

3.5.10 Voor opmerkingen over veiligheid, privacy en ethiek: zie par. 4 van dit advies.

3.6 *Andere RFID-beleidskwesties*

3.6.1 Behalve veiligheid, privacybescherming en ethiek komen ook radiospectrum, normen, gezondheids-, veiligheids- en milieuvraagstukken aan de orde in de beleidsdiscussie over RFID.

3.6.2 Met name de harmonisering van spectrumgebruiksvoorwaarden is van belang om de mobiliteit te vergemakkelijken en de kosten laag te houden. De Commissie heeft onlangs een beschikking vastgesteld (2006/808/EG) voor RFID-frequenties in de UHF-band. Deze toewijzing lijkt adequaat te zijn voor een periode van 3 à 10 jaar, maar mocht er extra spectrum nodig zijn, dan zal de Commissie maatregelen nemen overeenkomstig de bevoegdheid die zij op grond van de Radiospectrumbeschikking (676/2002/EG) bezit, hetgeen door het EESC wordt toegejuicht.

3.6.3 Een gestroomlijnde goedkeuring van internationale normen en harmonisering van regionale normen zijn dan ook van wezenlijk belang voor een soepele invoering van diensten. De relevante Europese normalisatie-instanties — CEN en ETSI — zijn hierbij volledig betrokken. De Commissie vraagt deze instanties, in samenwerking met het bedrijfsleven, ervoor te zorgen dat internationale en Europese normen voldoen aan de Europese eisen inzake privacybescherming, veiligheid,

([1]) Richtlijn 95/46/EG betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens.

([2]) Richtlijn 2002/58/EG betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie.

intellectuele-eigendomsrechten en machtigingsvraagstukken. Omdat industriële normen en intellectuele eigendomsrechten vaak samengaan, dringt het Comité er bij de Commissie op aan om het bedrijfsleven en de normalisatie-instanties tot snelle actie aan te sporen om te voorkomen dat de Europese RFID-toepassingen overafhankelijk worden van dure intellectuele eigendom die in andermans handen is.

3.6.4 Wat het milieu betreft, voldoet RFID aan de definitie van elektrische en elektronische apparatuur van de Richtlijn 2002/96/EG betreffende afgedankte elektrische en elektronische apparatuur (AEEA) en Richtlijn 2002/95/EG betreffende beperking van het gebruik van bepaalde gevaarlijke stoffen in elektrische en elektronische apparatuur (BGS). Op het gebied van de gezondheidszorg zijn daar de mogelijke gevolgen van elektromagnetische velden (EMV) voor de gezondheid van de mens. Elektromagnetische velden die verband houden met RFID-toepassingen hebben over het algemeen een lage sterkte. Maar gezien de algemene stijging in het aantal draadloze toepassingen zal de Commissie erop blijven toezien dat het rechtskader in acht wordt genomen, hetgeen door het EESC wordt toegejuicht.

4. **Opmerkingen**

4.1 Aangezien de Commissie haar aanbevelingen aan de lidstaten eind dit jaar zal publiceren, mag redelijkerwijs worden aangenomen dat zij de *status quo* op het gebied van gegevensbeveiliging en privacy zal handhaven. Concreet betekent dit dat de bestaande nationale instanties die over gegevensbescherming waken, ook verantwoordelijk zullen worden voor alles wat op het vlak van RFID met privacy en gegevensbescherming heeft te maken.

4.2 In haar mededeling heeft de Commissie o.a. aangekondigd een nieuwe groep van belanghebbenden te willen oprichten en raadplegen. Het Comité zou het onderhavige advies graag aan deze groep voorleggen.

4.3 RFID brengt de privacy en de burgerlijke vrijheden ernstig in gevaar:

a) RFID-tags kunnen worden aangebracht in/op voorwerpen en documenten zonder dat de ontvanger hier iets van merkt. Omdat radiogolven gemakkelijk en geluidloos door stof, plastic en ander materiaal heen gaan, kunnen RFID-tags die in kleding zijn genaaid of op voorwerpen zijn aangebracht die in handtassen, winkeltassen, koffers e.d. worden vervoerd, worden gelezen;

b) met een elektronische productcode kan elk voorwerp op aarde van een eigen, unieke ID worden voorzien. Het gebruik van unieke ID-nummers kan leiden tot een wereldwijd registratiesysteem waarbij elk voorwerp wordt geïdentificeerd en op het moment van verkoop of overdracht aan zijn koper of eigenaar wordt gekoppeld;

c) het gebruik van RFID vergt het opzetten van grote databanken met unieke tag-gegevens. Deze bestanden kunnen worden gekoppeld aan persoonlijke identificatiegegevens, vooral naarmate de geheugens en de verwerkingscapaciteit van computers toenemen;

d) tags kunnen vanaf een afstand worden gelezen, ook buiten het gezichtsveld, door lezers die onzichtbaar kunnen worden verwerkt in bijna elke omgeving waar mensen samenkomen. Lezers kunnen worden aangebracht in vloertegels, verwerkt in tapijt, verborgen in deuropeningen en verstopt in kasten, waardoor het voor een individu vrijwel onmogelijk wordt om erachter te komen wanneer hij of zij wordt gescand;

e) indien persoonlijke identiteit wordt gekoppeld aan unieke RFID-tagnummers, kunnen mensen zonder dat zij het weten of zonder dat zij hiervoor toestemming hebben verleend worden gevolgd of geprofileerd;

f) een wereld waarin RFID-lezers een allesomvattend, wereldwijd netwerk vormen is niet ondenkbaar. Voor een dergelijk netwerk zijn niet overal lezers nodig. In Londen worden alle auto's die het centrum van Londen binnenkomen voor congestieheffing met relatief weinig, strategisch geplaatste camera's gefotografeerd. Een netwerk van strategisch geplaatste RFID-lezers kan op dezelfde manier worden opgezet. Dat mag niet gebeuren.

4.4 In het 7e kaderprogramma voor O&O heeft de Commissie al richtsnoeren opgenomen voor de ethische toepassing van technologie voor wat gegevensbescherming en privacy betreft (zie „Guide for Applicants for collaborative projects", blz. 54) ([3]). Uit RFID blijkt bij uitstek welk effect de zich steeds verder ontwikkelende technologie heeft op het wettelijk recht op de door iedereen als vanzelfsprekend beschouwde privacy bij het verzamelen en delen van gegevens. Privacyproblemen ontstaan wanneer unieke identificeerbare gegevens m.b.t. een persoon of personen worden verzameld en opgeslagen, in digitale vorm of anderszins. Slecht of geen toezicht op het vrijgeven van gegevens kan de privacy in het gedrang brengen. De gegevens die het meest privacygevoelig zijn, betreffen gezondheid, strafblad, financiële situatie, genetische informatie en verblijfplaats. RFID richt zich vooral op het vaststellen van de verblijfplaats.

4.5 In de richtsnoeren voor het omgaan met gegevensbeveiliging en privacy ([4]) heeft de Commissie acht dwingende beginselen van goede praktijken vastgelegd. Gegevens:

— moeten eerlijk en rechtmatig worden verwerkt;

— moeten voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verkregen;

— moeten adequaat, terzake dienend en niet buitensporig zijn;

— moeten nauwkeurig zijn;

— mogen niet langer worden bewaard dan noodzakelijk is;

— moeten worden verwerkt overeenkomstig de rechten van de betrokkene;

— moeten beveiligd zijn;

— mogen niet zonder adequate bescherming worden doorgegeven aan andere landen.

In deze richtsnoeren wordt een antwoord gegeven op alle vragen betreffende privacy en gegevensbeveiliging i.v.m. de toepassingen van RFID.

([3]) http://cordis.europa.eu/fp7/dc/index.cfm?fuseaction=UserSite.CooperationDetailsCallPage&call_id=11.

([4]) Richtlijn 95/46/EG betreffende de bescherming van persoonsgegevens, art. 6.

4.6 Volgens het EESC luiden de basisbeginselen van goede praktijken als volgt:

— RFID-gebruikers moeten hun beleid en praktijken openbaar maken en er mogen geen geheime databanken betreffende persoonsgegevens zijn.

— Iedereen heeft het recht te weten of producten in winkels RFID-tags of -lezers bevatten. Indien er in winkels sprake is van het lezen van tags, moet dit op voor alle partijen transparante wijze gebeuren.

— RFID-gebruikers moeten mededelen voor welke doeleinden tags en lezers worden gebruikt. Alleen de informatie die noodzakelijk is voor het beoogde doel, mag worden verzameld.

— RFID-gebruikers zijn verantwoordelijk voor de toepassing van de technologie en moeten erop toezien dat e.e.a. binnen de grenzen van de wetgeving en richtlijnen inzake gegevensbeveiliging gebeurt. Zij zijn ook verantwoordelijk voor de veiligheid en volledigheid van het systeem en zijn databanken.

4.7 Hoe deze principes in de praktijk moeten worden gebracht, is nog niet duidelijk. In het gunstigste geval geven alle bedrijven die met de consument zaken doen, zoals winkeliers, kaartverkopers, toegangscontroleurs of vervoerders hun klanten een soort garantie dat deze principes in acht zullen worden genomen, een soort klantenhandvest. Een dergelijk handvest zou alle beginselen van goede praktijken m.b.t. gegevensbescherming zoals omschreven in par. 4.5 kunnen bevatten. Daarnaast stelt het Comité de volgende richtsnoeren voor:

a) Handelaren mogen hun klanten niet verplichten om te accepteren dat de producten die zij kopen actieve of passieve tags bevatten. Als alternatief kunnen de tags op de verpakking worden aangebracht of kan gebruik gemaakt worden van verwijderbare tags (zoals bij prijskaartjes).

b) Klanten moeten de tags op de voorwerpen die zij in hun bezit hebben kunnen verwijderen of de-activeren.

c) RFID mag in principe niet worden gebruikt om personen op te sporen. Het opsporen van mensen is onaanvaardbaar, of dat nu bijvoorbeeld via kleding, goederen, kaarten of andere dingen gebeurt.

d) RFID mag nooit worden gebruikt op een manier die de anonimiteit kan opheffen of beperken.

e) De verantwoordelijke instantie zou duidelijk moeten maken dat c) en d) alleen zijn toegestaan in uitzonderlijke omstandigheden en met voorafgaande, formele kennisgeving aan de instantie.

4.8 Op het bovenstaande kunnen bepaalde uitzonderingen worden toegestaan wanneer

— natuurlijke personen gebruik maken van de keuzemogelijkheid om de tags te behouden voor persoonlijke doeleinden;

— natuurlijke personen ermee instemmen dat hun gangen kunnen worden nagegaan wanneer zij zich in een kritische omgeving bevinden, zoals streng beveiligde openbare en private gebouwen en instellingen;

— natuurlijke personen ervoor kiezen om toepassingen te gebruiken waarmee zij, net als door het gebruik van mobiele telefoons, ATM-kaarten, internetadressen enz., kunnen worden gelokaliseerd en geïdentificeerd.

De verantwoordelijke instantie moet van dergelijke uitzonderingen in kennis gesteld worden.

4.9 Een toepassing waarvoor een algemene uitzondering zou kunnen gelden, is het traceren van mensen of goederen in een tijdelijke situatie. In het luchtvervoer kan bagage bij het inchecken van een tag worden voorzien om de bagagebehandeling veiliger en betrouwbaarder te maken; door het „merken" van passagiers kan de stiptheid van vliegbewegingen worden verbeterd en kunnen veiligheidsprocedures worden bespoedigd. Een andere toepassing is eventueel het traceren van patiënten die voor een operatie in het ziekenhuis zijn opgenomen. Dergelijke toepassingen zijn alleen aanvaardbaar indien wordt gewaarborgd dat de tags aan het eind van de tijdelijke situatie worden vernietigd.

4.10 RFID is nog niet uitontwikkeld, dus nog niet alle mogelijkheden zijn bekend. Enerzijds kan RFID van onschatbare waarde zijn voor onze technologische beschaving, maar anderzijds kan het de grootste bedreiging ooit voor privacy en vrijheid zijn. Het Comité is van mening dat de ontwikkeling van RFID-toepassingen moet doorgaan maar dat zulks volgens strikte ethische regels en zonder aantasting van privacy, vrijheid en gegevensbescherming moet gebeuren.

4.11 Kortom, waar RFID-toepassingen worden toegestaan, moet het gebruik ervan volkomen transparant zijn voor alle betrokkenen. Toepassingen die de afhandeling van goederen verbeteren, zijn algemeen aanvaardbaar. Toepassingen waarbij mensen van tags worden voorzien, zijn in het algemeen onaanvaardbaar, behalve in tijdelijke situaties. Toepassingen die mensen en goederen met elkaar verbinden, kunnen aanvaardbaar zijn voor marketingdoeleinden. Toepassingen waarbij mensen worden geïdentificeerd aan de hand van de goederen die zij hebben gekocht, zijn over het algemeen onaanvaardbaar. Sommige toepassingen zijn sowieso onaanvaardbaar in een vrije maatschappij en mogen nooit worden toegestaan. De dwingende noodzaak om privacy en anonimiteit in stand te houden moet de kern van de aanbeveling van de Commissie aan de lidstaten zijn.

Brussel, 11 juli 2007.

De voorzitter

van het Europees Economisch en Sociaal Comité

Dimitris DIMITRIADIS