Det Europæiske Økonomiske og Sociale Udvalgs udtalelse om »Radiofrekvensidentifikation (RFID)«

(2007/C 256/13)

I et brev af 26. februar 2007 anmodede Kommissionen under henvisning til EF-traktatens artikel 262 Det Europæiske Økonomiske og Sociale Udvalg om at udarbejde en udtalelse om: *Radiofrekvensidentifikation (RFID)*.

Det forberedende arbejde henvistes til EØSU's Sektion for Transport, Energi, Infrastruktur og Informationssamfundet, som udpegede Peter Morgan til ordfører. Sektionen vedtog sin udtalelse den 19. juni 2007.

Det Europæiske Økonomiske og Sociale Udvalg vedtog på sin 437. plenarforsamling den 11.-12. juli 2007, mødet den 11. juli, følgende udtalelse med 138 stemmer for, 1 imod og 6 hverken for eller imod:

1. **Konklusioner og henstillinger**

1.1 Radiofrekvensidentifikation (RFID) er en betydningsfuld teknologi, som med tiden vil blive særdeles vigtig. Dens nuværende og fremtidige anvendelse vil kunne bidrage til positive forbedringer i en lang række forretningsgange såvel i den offentlige som i den private sektor og medføre betragtelige fordele både for de enkelte borgere og for virksomheder. RFID vil også kunne stimulere en kraftig udvikling af internetapplikationer og muliggøre, hvad et FN-organ har beskrevet som »tingenes internet«. Men, medmindre RFID er under nøje kontrol, kan den risikere at medføre overtrædelse af lovgivningen om beskyttelse af personoplysninger og krænkelser af borgerrettigheder og blive en trussel mod enkeltpersoners og virksomheders sikkerhed.

1.2 Meddelelsens fulde titel er »Radiofrekvensbaseret identifikation (RFID) i Europa: elementer til en politisk ramme.« Kommissionen har afholdt en omfattende høring, der har dannet grundlag for meddelelsen. EØSU opfordres nu til at afgive en sonderende udtalelse. Med udgangspunkt i reaktionerne på meddelelsen vil Kommissionen, ved årets udgang, fremsætte en henstilling til medlemsstaterne. En eventuel lovgivning, som vil tage længere tid, kommer på et senere tidspunkt. Denne udtalelse skal fokusere på henstillingens indhold.

1.3 Til at hjælpe med udarbejdelsen af sine henstillinger har Kommissionen besluttet at nedsætte en interessentgruppe, der skal fungere som en slags tænketank. EØSU ville gerne have mulighed for at fremlægge sin udtalelse for denne interessentgruppe.

1.4 EØSU støtter de foranstaltninger, som Kommissionen foreslår på områderne for radiospektrum, standarder, sundhed, sikkerhed og miljø, og understreger, at det haster med et effektivt industrielt bidrag til forummet for standarder.

1.5 Eftersom Kommissionen vil offentliggøre sine henstillinger til medlemsstaterne ved årets udgang, er der god grund til at formode, at den vil videreføre den nuværende infrastruktur for datasikkerhed og sikring af privatlivets fred. Det betyder, at de allerede eksisterende databeskyttelsesinstanser i de enkelte medlemsstater også bliver ansvarlige for beskyttelse af privatlivets fred og databeskyttelse i forbindelse med RFID-anvendelser. Udtalelsen fokuserer på disse emner.

1.6 RFID udgør en alvorlige trussel mod privatlivets fred og borgerrettighederne:

— RFID-tags kan indføjes i/påsættes genstande og dokumenter, uden den persons vidende, der kommer i besiddelse af disse ting. Da radiobølger bevæger sig let og lydløst gennem stof, plastik og andre materialer, kan det lade sig gøre at aflæse RFID-tags, der er syet ind i tøj eller hæftet på ting, der opbevares i pengepungen, indkøbstasker, kufferter og lignende.

— Den elektroniske produktkode kan gøre det muligt at give enhver ting på jorden sit helt eget ID-nummer. Anvendelsen af unikke ID-numre kunne føre til oprettelsen af et verdensomspændende databasesystem, hvor alle fysiske objekter kan identificeres og forbindes med deres køber eller ejer ved salgs- eller overdragelsesstedet.

— Udbredelse af RFID-teknologien kræver oprettelse af massive databaser, der indeholder unikke tag-data. Denne registrering kan kædes sammen med personoplysninger, efterhånden som computeres lagrings- og behandlingskapacitet udvides.

— RFID-tags behøver ikke befinde sig inden for synsfeltet, men kan aflæses på afstand af scannere, der kan installeres usynligt næsten overalt, hvor mennesker færdes. RFID-aflæsere kan lægges ned i gulvfliser, væves ind i gulvtæppet, skjules i dørkarmen eller gemmes på hylderne, så det rent faktisk er umuligt for den enkelte at vide om han/hun scannes.

— Hvis personoplysninger er knyttet til unikke RFID-tags, kan man spore personer eller udarbejde en profil på dem uden deres vidende eller samtykke.

— Man kunne godt forestille sig en verden, hvor RFID-aflæsere udgør et omsiggribende globalt netværk. Et sådant netværk kræver ikke scannere overalt. Afgifter for trafikbelastning i London kan med forholdsvist få strategisk placerede kameraer spore samtlige biler, der kører ind i Londons centrum. På samme måde kunne man oprette et netværk af strategisk placerede RFID-aflæsere. Det må ikke få lov at ske.

1.7 Konsekvenserne af disse trusler er følgende:

— RFID-brugere skal offentliggøre deres politikker og praksis, og der bør ikke findes hemmelige databaser med personoplysninger.

— Den enkelte har ret til at vide, hvornår varer i detailhandelen er udstyret med RFID-tags eller -aflæsere. Enhver tag-aflæsning, der foregår i detailhandlen, bør foregå på gennemskuelig vis for alle parter.

— RFID-brugere skal oplyse om formålet med anvendelse af tags og aflæsere. Indsamling af oplysninger bør begrænses til, hvad der er nødvendigt for det pågældende formål.

— RFID-brugere bærer ansvaret for anvendelsen af teknologien og for, at sikkerhedslovgivningen og retningslinjerne overholdes. De bærer også ansvaret for systemets og databasens sikkerhed og integritet.

1.8 Hvordan disse principper skal omsættes i praksis er et åbent spørgsmål. Ideelt set skulle enhver virksomhed, som indgår forretningsaftaler med kunder ved detailhandel, billetudstedelse, adgangskontrol eller transportydelser, udstede kunderne en form for garanti for, at principperne vil blive fulgt, en form for kundecharter. Et sådant charter kunne indeholde de principper for god praksis vedrørende databeskyttelse, som beskrives i punkt 4.5. Desuden foreslår EØSU følgende retningslinjer:

a) Det bør være forbudt for de handlende at presse eller tvinge kunderne til at acceptere aktive eller passive tags i de produkter, de køber. En mulighed kunne være, at tags placeres på emballagen eller at man anvender tags, der kan fjernes på samme måde som prismærker.

b) Kunderne skal frit kunne fjerne eller desaktivere tags, der er placeret på genstande i deres besiddelse.

c) RFID bør, som hovedregel, ikke anvendes til at spore personer. Sporing af mennesker er upassende, uanset om det sker gennem f.eks. tøj, varer, billetter eller andre ting.

d) RFID bør aldrig anvendes med henblik på at afskaffe eller indskrænke anonymitet.

e) Den ansvarlige myndighed bør give klare instrukser om, at (c) og (d) kun kan tillades under særlige omstændigheder og efter forudgående formel underretning af myndigheden.

1.9 Enkelte undtagelser fra ovenstående retningslinjer kan komme på tale, når:

— enkeltpersoner i egen interesse vælger at bibeholde aktive tags;

— enkeltpersoner indvilliger i at blive sporet i kritiske omgivelser, som f.eks. sikrede private og offentlige anstalter og institutioner;

— enkeltpersoner vælger at benytte applikationer, som lokaliserer og identificerer dem på samme måde som de allerede nu lokaliseres og identificeres ved brug af mobiltelefoner, betalingskort, internetadresser osv.

Enhver af disse undtagelser skal oplyses til den ansvarlige myndighed.

1.10 RFID er ingen færdigudviklet teknologi, så vi kender endnu ikke dens fulde potentiale. På den ene side indebærer den måske ufattelige fordele for vores teknologiske civilisation, på den anden side er det måske vor tids største teknologiske trussel mod privatlivets fred og friheden. EØSU er af den overbevisning, at RFID-systemanvendelser bør udvikles i overensstemmelse med strenge etiske regler om privatlivets fred, frihed og datasikkerhed, men systemudviklingen bør fortsætte under forudsætning af, at nødvendige forholdsregler træffes.

1.11 Kort sagt bør implementeringen være fuldt ud gennemskuelig for alle involverede parter, når RFID-applikationer er tilladte. Generelt er systemanvendelser, der letter håndteringen af varer, acceptabel. Systemanvendelser, der medfører, at mennesker udstyres med tags, kan som hovedregel kun accepteres i kortere perioder. Systemanvendelser, som forbinder mennesker til varer, kan accepteres med henblik på markedsføring. RFID-anvendelser, som identificerer mennesker gennem varer, de har købt, er som hovedregel uacceptable. Derudover passer visse systemanvendelser slet ikke ind i et frit samfund og bør derfor aldrig tillades. Det helt centrale i Kommissionens henstilling til medlemsstaterne må være det bydende behov for at værne om privatlivets fred og anonymiteten.

2. **Hvad er RFID og hvorfor er det så vigtigt?**

2.1 RFID er en teknologi, der muliggør automatisk identifikation og datafangst ved brug af radiofrekvenser. Det iøjnefaldende ved denne teknologi er, at enhver genstand, eller for den sags skyld ethvert dyr eller menneske, kan udstyres med en elektronisk tag, der indeholder en entydig identitetsmarkør og andre oplysninger, som kan aflæses trådløst.

2.2 Disse tags består af et elektronisk kredsløb, som opbevarer data, samt en antenne, som videresender dataene gennem radiobølger. En RFID-scanner aflæser chippene for at indhente de lagrede oplysninger. Så snart chip-læseren udsender radiobølger, vil alle tags inden for dens rækkevidde blive afkodet. Der skal bruges software til at kontrollere RFID-læseren og indsamle og filtrere informationen.

2.3 Der findes forskellige former for RFID-systemer. Tags kan enten være aktive eller passive. Aktive tags indeholder et integreret batteri til at drive det interne kredsløb og til at frembringe radiobølger. De kan endda transmittere, selvom der ikke er nogen RFID-læser i nærheden. Passive tags er energidrevne gennem de radiobølger, RFID-læseren transmitterer og har ikke egen energiforsyning. RFID-tags kan være »read-only« eller »read-write«. Read only-tags er billigere at fremstille og anvendes i de fleste aktuelle systemanvendelser.

2.4 RFID-systemets rækkevidde afhænger af radiofrekvensen, RFID-aflæserens energiforsyning og materialet mellem taggen og RFID-aflæseren. Den kan være op til nogle få meter for passive systemer, men overstige mere end 100 meter for aktive systemer.

2.5 RFID er det nederste trin i den trådløse teknologis hierarki. Rangerende efter hvor stor afstand signalet spænder over, indtager satellitkommunikationssystemer som GPS førstepladsen. Dernæst følger vidtrækkende mobiltelefoniteknologier, som f.eks. GSM og GPRS, derefter kortere rækkende signaler inden for bygninger som Wi-Fi, så personlige netværker som Bluetooth og til sidst altså, RFID. Hver enkelt af disse teknologier er specifikke og selvstændige, så der altså ikke er nogen risiko for, at satellitsystemer aflæser RFID-tags. Alligevel kan data overføres mellem de respektive systemer gennem anordninger, som f.eks. mobiltelefoner.

2.6 Herunder nævnes nogle eksempler på de potentielle fordele ved RFID-teknikken:

— For borgerne kan den øge sikkerheden (hvad angår fødevarer, sundhed, bekæmpelse af forfalskninger), bekvemmeligheden (kortere supermarkedskøer, mere præcis og pålidelig håndtering af bagage i lufthavne, automatiseret betaling) og forbedret patientpleje, navnlig af kroniske sygdomme som demens.

— På transportområdet forventes den at bidrage til effektivisering, øget sikkerhed og ydelser af høj kvalitet for mennesker og varer.

— På sundhedsområdet kan RFID være med til at højne kvaliteten af plejen og øge patienternes sikkerhed og sikre bedre overholdelse af medicineringsforskrifter samt forbedre logistikken. Der arbejdes i øjeblikket på at kunne tilføre individuelle piller RFID-tags.

— I detailhandelen kunne RFID være med til at mindske forsyningsmangler, lagerbeholdning, og tyveri.

— I mange brancher, hvor mærkevareforfalskning er særligt udbredt, kan RFID hjælpe med til at finde frem til de steder, hvor ulovlige varer når ind i forsyningskæden.

— RFID-mærkning forventes også at forbedre sorteringen og genanvendelsen af produktdele og materialer, hvilket kan føre til forbedring indenfor affaldsbehandling og bæredygtig udvikling.

2.7 Mange af RFID-systemets aspekter kan illustreres gennem dets anvendelse i bøgers livscyklus. Den enorme mængde bøger, der udkommer, udgør et logistisk mareridt for forlag, distributører, biblioteker og detailhandlere. Bortset fra forsyningskædelogistik skal man kunne spore bøgerne, så snart de er blevet placeret på hylderne, så de både kan lokaliseres og skiftes ud. Derudover skal biblioteker kunne kontrollere udlånscyklus, mens køberne kan have svært ved at holde rede på deres egne bøger. RFID-tags på bøger giver løsningen på alle disse problemer. Kontrol med biblioteksudlån kan overføres til ethvert andet system, hvor ting genbruges eller lejes ud.

2.8 For at illustrere de risici, der er forbundet med denne teknologi, er her et uddrag fra en IBM patentansøgning (20020615758) fra november 2002. Den vedrører identificering og sporing af personer, der anvender RFID-mærket udstyr.

> »En metode og et system til identifikation og sporing af personer, der anvender RFID-mærket udstyr, som bæres af personerne. Registre over tidligere foretagede indkøb indsamles for hver enkelt person, der handler i en detailforretning, gennem salgsregistreringssystemer og lagres i en indkøbssdatabase. Når en person, der bærer eller har noget på, der er udstyret med en RFID-tag, går ind i forretningen eller et andet afgrænset område, scannes etiketterne på den pågældende person af den i lokalet opstillede RFID-scanner og informationerne på RFID-taggen aflæses. Den indsamlede RFID-tag information sammenholdes med oplysninger om tidligere indkøb, der er lagret i indkøbsdatabasen i overensstemmelse med kendte korrelationsalgoritmer. På baggrund af korrelationsresultaterne kan personens nøjagtige identitet eller visse af personens kendetegn fastlægges. Informationen bruges til at overvåge personens bevægelse gennem forretningen eller andre områder.«

American Express patentansøgning nummer 20050038718 går ud på det samme.

2.9 RFID er helt klart andet og mere end en elektronisk stregkode. De væsentligste forskelle fremgår af ovenstående uddrag:

a) RFID-taggen indeholder ikke blot en varebeskrivelse, men også en diskret identitetsmarkør som igen kan identificere køberen.

b) Taggen behøver ikke være en fysisk mikrochip. Kredsløbene kan trykkes direkte på de fleste materialer, som f. eks. tøj.

c) Taggen kan forblive aktiv efter salget, så den kan genaflæses kontinuerligt.

d) RFID-aflæserne findes ikke kun på salgsstedet, de kan befinde sig hvor som helst og ikke kun i detailhandelens lokaler.

e) Korrelationen via en database indfører en ny dimension i dataindsamling, privatlivets fred og datasikkerhed.

2.10 Hvorvidt en tag skal forblive aktiv efter at have forladt detailforretningen, kan diskuteres. På den ene side er det en trussel mod privatlivets fred. På den anden side kunne det være en fordel for køberen. For eksempel kan RFID-aflæsere være en hjælp til at holde rede på hjemmets vinkælder, køleskabets indhold, garderoben og biblioteket. Den logiske følge bør derfor være, at den enkelte selv træffer valget, men teknologien og dens anvendelse skal tilbyde personen dette valg.

2.11 RFID kan bruges til meget mere end blot detail produktidentifikation. EØSU's adgangskort er et RFID-system. Metrosystemet i London anvender i udbredt grad RFID-kort til betaling og adgang. Kreditkort vil snart indeholde en RFID-anordning til betaling af mindre beløb uden brug af pinkode. RFID-etiketter anvendes til opkrævning af motorvejsafgift og identifikation af føreren af et køretøj. Adgangen til skilifte kontrolleres på visse europæiske skisportssteder med RFID-etiketter, som ligger i lommen på skidragten. Deres ordfører har hver dag tre RFID-kort og en RFID-etiket på sig. Hans hund identificeres gennem en RFID-chip, der er implanteret under huden. Sådanne chips er ved at være meget udbredt i hele verden til mærkning af dyr, og til at spore fødevarer. Der er ikke lang vej til at RFID-mærke kriminelle og problematiske patienter på samme måde som hunde.

2.12 Det adgangskort, man anvender i EØSU, er en mild form for RFID-systemanvendelse. Identitet bliver en så meget desto større udfordring, når RFID-tags indsys i arbejdstøj eller uniformer, så den uniformerede persons bevægelser kan følges kontinuerligt af strategisk placerede scannere på arbejdspladsen. EØSU medgiver dog, at dette kan være ønskeligt i visse tilfælde, f.eks. af sikkerhedsgrunde. Men at spore, hvor en person befinder sig, vil, hvis det sker uden passende beskyttelsesforanstaltninger, være en alvorlig krænkelse af privatlivets fred og forudsætter en god begrundelse og en meget omhyggelig kontrol.

2.13 Som et bizart varsel for fremtidige anvendelser, rapporterer *The Economist*, at adgangsbilletten til VIP-området i Baja Beach Club i Barcelona er en mikrochip indopereret i stamgæstens arm. Chippen, som er på størrelse med et riskorn og belagt med glas og silikone, bruges til at identificere folk, når de ankommer og betaler for drinks. Den implanteres af en sygeplejerske under lokalbedøvelse. I bund og grund er det en RFID-tag.

3. **Resumé af meddelelsen**

3.1 RFID vækker politisk interesse, fordi det kan blive en ny motor for vækst og beskæftigelse og dermed et vægtigt bidrag til Lissabon-strategien, hvis blot innovationsbarriererne kan overvindes.

3.2 Kommissionen gennemførte en offentlig høring om RFID i 2006, som satte fokus på forventningerne til teknikken med udgangspunkt dér, hvor den er blevet taget i brug på et tidligt tidspunkt, men som også afslørede borgernes betænkeligheder ved RFID-anvendelser, der indebærer identifikation og/eller sporing af mennesker.

3.3 En fortsat udvikling og udbredt anvendelse af RFID kan gøre informations- og kommunikationsteknologien til en endnu stærkere drivkraft for innovation og økonomisk vækst.

3.4 Der er brug for klare og forudsigelige juridiske og politiske rammer for at gøre denne nye teknik acceptabel for brugerne. Da RFID-teknikken af natur er grænseoverskridende, må rammerne sikre ensartethed på hele det indre marked.

3.5 *Sikkerhed, privatlivets fred og etik.*

3.5.1 Der er alvorlig bekymring for, at denne altgennemtrængende basisteknologi kan true privatlivets fred: RFID-teknikken kan bruges til at indsamle oplysninger, der er direkte eller indirekte forbundet med en identificerbar eller identificeret person, og derfor anses for at være personoplysninger. RFID-tags kan indeholde personoplysninger. RFID-teknologi kan anvendes til at spore eller følge folks bevægelser eller til at tegne en profil af folks adfærd. RFID kan i givet fald blive en privatlivskrænkende teknologi. Der er ytret betænkelighed ved mulige krænkelser af de grundlæggende værdier og privatlivets fred og øget overvågning, navnlig på arbejdspladser, med diskrimination, udstødelse og måske fyring til følge.

3.5.2 Brugen af RFID skal naturligvis være socialt og politisk acceptabel, etisk forsvarlig og lovlig. Det store økonomiske og sociale udbytte, RFID kan give, kommer kun, hvis der findes effektive garantier for databeskyttelse og privatlivets fred og de dertil hørende etiske forhold, som er centrum i debatten om borgernes accept af RFID.

3.5.3 Fællesskabets rammebestemmelser om databeskyttelse og privatlivets fred i Europa er udformet, så de skulle være robuste over for innovation. Beskyttelsen af personoplysninger er omfattet af det generelle databeskyttelsesdirektiv ([1]), som gælder for alle teknologier, også RFID. Det generelle databeskyttelsesdirektiv suppleres af e-databeskyttelsesdirektivet ([2]). Ifølge disse direktiver har medlemsstaternes myndigheder pligt til at overvåge, at indførelsen af RFID-anvendelser sker i overensstemmelse med lovgivningen om privatlivets fred og databeskyttelse. Det kan derfor være nødvendigt at give detaljerede retningslinjer for den praktiske gennemførelse af en teknik som RFID og at udarbejde adfærdskodekser i den forbindelse.

3.5.4 Hvad sikkerheden angår, skal erhvervslivet, medlemsstaterne og Kommissionen i fællesskab gøre en indsats for at opnå dybere indsigt i de systemimmanente problemer og dermed forbundne sikkerhedsrisici ved at tage RFID-teknologier og -systemer i brug i massevis. En vigtig del af svaret på ovennævnte udfordringer kommer til at bestå i udarbejdelse af specifikationer og vedtagelse af konstruktionskriterier, der forebygger risici for privatlivets fred og sikkerheden, ikke kun teknologisk, men også organisatorisk og i forbindelse med forretningsprocesser. Derfor må der foretages en grundig lønsomhedsanalyse af specifikke sikkerheds- og privatlivsrelaterede risici, før der vælges RFID-systemer og udbredes RFID-anvendelser.

3.5.5 Der er bekymring for åbenheden og neutraliteten i de databaser, der skal registrere de entydige identitetsmarkører, som er kernen i RFID-systemet, samt lagringen og håndteringen af de indsamlede data, herunder tredjeparters udnyttelse af dem. Spørgsmålet har stor betydning, for RFID kommer til at bære en ny bølge i internettets udvikling, som vil ende med at danne et trådløst væv af milliarder af smarte chips og avancerede sensorer i en verdensomspændende kommunikationsinfrastruktur. Denne nye fase i internettets udvikling kaldes »tingenes internet«.

3.5.6 Dette registrerings- og benævnelsessystem i det fremtidige »tingenes internet« skal sikre mod sammenbrud eller utilsigtet brug, som kunne skabe kaos. Det må ikke falde i hænderne på særinteresser, der kunne bruge disse databaser og systemer til deres egne formål. Hensynet til sikkerhed, etik og privatlivets fred bør varetages for alle interessenter, fra enkeltpersoner til selskaber, som har følsomme forretningsinformationer i RFID-baserede forretningsprocesser.

3.5.7 Når der skal konstrueres et RFID-informationssystem, skal der tages hensyn til kravene fra både de parter, der aktivt medvirker til at oprette det (f.eks. virksomheder, myndigheder eller sygehuse), og slutbrugerne, der udsættes for det (borgere, forbrugere, patienter og ansatte). Da slutbrugerne normalt ikke inddrages i teknologiens designstadie, vil Kommissionen give støtte til, at en central ekspertgruppe med repræsentanter for alle parter udarbejder et sæt retningslinjer for de enkelte anvendelser (adfærdskodeks, god praksis). Ved udgangen af 2007 vil Kommissionen udstede en henstilling om, hvilke principper myndighederne og andre berørte parter bør følge i forbindelse med brug af RFID.

3.5.8 Derudover vil Kommissionen overveje at indføje bestemmelser i det kommende forslag om ændring af e-databeskyttelsesdirektivet og sideløbende hermed tage hensyn til bidrag fra den kommende RFID-interessentgruppe, Artikel 29-Arbejdsgruppen om Databeskyttelse og andre relevante initiativer, f.eks. Den Europæiske Gruppe vedrørende etik inden for naturvidenskab og ny teknologi. På det grundlag vil Kommissionen vurdere behovet for yderligere lovgivning til at værne om data- og privatlivsbeskyttelse.

3.5.9 Kommissionen vil holde nøje øje med udviklingen hen imod et »tingenes internet«, hvor RFID forventes at komme til at spille en stor rolle. Ved udgangen af 2008 vil Kommissionen udsende en meddelelse, der analyserer forløbet og virkningerne af en sådan udvikling med særlig vægt på spørgsmålene om privatlivets fred, tillid og regulering. Den vil vurdere, hvilke strategiske valgmuligheder der foreligger, og om det er nødvendigt at foreslå flere lovgivningstiltag for at varetage databeskyttelses- og privatlivshensyn og sikre andre almindelige retsprincipper.

3.5.10 Bemærkninger til emnerne sikkerhed, privatlivets fred og etik er samlet i udtalelsens punkt 4.

3.6 *Andre politiske RFID-spørgsmål*

3.6.1 Bortset fra hele området »sikkerhed, privatlivets fred og etik« rejser RFID-systemet andre politiske spørgsmål såsom frekvensressourcer, standarder, sundhed, sikkerhed og miljø.

3.6.2 Det er vigtigt at harmonisere vilkårene for frekvensanvendelse for at muliggøre uhindret mobilitet og lave omkostninger. Kommissionen vedtog for nylig en beslutning (2006/808/EF) om RFID-frekvenser i UHF-båndet. Denne fordeling anses for at være tilstrækkelig inden for en tre- til tiårig tidshorisont, men såfremt der skulle opstå et behov for flere frekvensressourcer, vil Kommissionen handle derefter og anvende sine beføjelser under radiospektrumsafgørelsen (676/2002/EF). EØSU accepterer denne holdning.

3.6.3 Strømlinet vedtagelse af nye internationale ISO-standarder og harmonisering af regionale standarder er således afgørende for en uhindret ibrugtagning af tjenesterne. De relevante europæiske standardiseringsorganer — CEN og ETSI — er fuldt ud involveret. Kommissionen opfordrer disse organer til i samarbejde med industrien at sikre, at udviklingsstandarderne opfylder de europæiske krav, navnlig hvad angår privatlivet fred, sikkerhed, intellektuel ejendomsret og licensspørgsmål. Eftersom

([1]) Direktiv 94/46/EØF om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger.
([2]) Direktiv 2002/58/EF om behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor.

industrinormer og enerettigheder ofte hænger sammen, opfordrer EØSU Kommissionen til at gøre, hvad den kan, for at få industrien og standardiseringsorganerne til at skynde sig at forhindre, at europæiske systemanvendelser af RFID bliver alt for afhængig af andres dyre intellektuelle ejendomsrettigheder.

3.6.4 Hvad miljøet angår, omfattes RFID-udstyr fuldt ud af direktivet om affald af elektrisk og elektronisk udstyr og direktivet om begrænsning af anvendelsen af visse farlige stoffer i elektrisk og elektronisk udstyr. For så vidt angår sundheden, kan der i givet fald være et problem med elektromagnetiske felter i forbindelse med RFID-udstyr. Elektromagnetiske felter i forbindelse med RFID-anvendelser er i almindelighed svage og derfor forventes arbejdstagernes og den brede offentligheds udsættelse herfor at ligge et godt stykke under de nugældende grænser. Set i lyset af den sideløbende vækst i trådløst udstyr vil Kommissionen dog fortsat holde øje med overholdelsen af lovrammerne. EØSU accepterer denne holdning.

4. **Bemærkninger**

4.1 Eftersom Kommissionen vil offentliggøre sine henstillinger til medlemsstaterne ved årets udgang, er der god grund til at formode, at den vil videreføre den nuværende infrastruktur for datasikkerhed og sikring af privatlivets fred. Det betyder, at de allerede eksisterende databeskyttelsesinstanser i de enkelte medlemsstater også bliver ansvarlige for beskyttelse af privatlivets fred og databeskyttelse i forbindelse med RFID-anvendelser.

4.2 Kommissionen har i sin meddelelse bl.a. slået fast, at den vil nedsætte og rådføre sig med en ny interessentgruppe. EØSU vil gerne fremlægge nærværende udtalelse for denne gruppe.

4.3 RFID udgør en alvorlige trussel mod privatlivets fred og borgerrettighederne:

a) RFID-tags kan indsættes i, eller påsættes genstande og dokumenter uden at den person, der kommer i besiddelse af disse ting, ved det. Da radiobølger bevæger sig let og lydløst gennem stof, plastik og andre materialer kan det lade sig gøre at aflæse RFID-tags, som er syet fast i tøj eller påsat ting, der opbevares i pengepungen, indkøbsposer, kufferter og lignende.

b) Den elektroniske produktkode kan gøre det muligt at give enhver ting på jorden sit helt eget ID-nummer. Anvendelsen af unikke ID-numre kunne føre til oprettelsen af et verdensomspændende databasesystem, hvor alle fysiske objekter kan identificeres og forbindes med deres køber eller ejer ved salgs- eller overdragelsesstedet.

c) Udbredelsen af RFID-teknologien kræver oprettelse af massive databaser, der indeholder unikke tag-data. Denne registrering kan kædes sammen med personoplysninger, efterhånden som computeres lagrings- og behandlingskapacitet udvides.

d) RFID-tags er ikke begrænset til synsfeltet og kan aflæses på afstand af scannere, der kan installeres usynligt næsten overalt, hvor mennesker færdes. RFID-aflæsere kan lægges ned i gulvfliser, væves ind i gulvtæppet, skjules i dørkarmen eller gemmes på hylderne, så det rent faktisk er umuligt for den enkelte at vide, hvornår han/hun scannes.

e) Hvis personoplysninger knyttes til unikke RFID-tags, kan man spore personer eller udarbejde en profil på dem uden deres vidende eller samtykke.

f) Man kunne godt forestille sig en verden, hvor RFID-aflæsere udgør et omsiggribende globalt netværk. Et sådant netværk kræver ikke scannere overalt. Afgifter for trafikbelastning i London kan med forholdsvist få strategisk placerede kameraer spore samtlige biler, der kører ind i Londons centrum. På samme måde kunne man oprette et netværk af strategisk placerede RFID-tagaflæsere. Det må ikke få lov at ske.

4.4 I det 7. F&U-rammeprogram har Kommissionen allerede vejledt om den etiske anvendelse af teknologien, da den har betydning for datasikkerhed og privatlivets fred (»vejledning for ansøgere« til samarbejdsprojekter, p. 54) ([3]). RFID er et glimrende eksempel på den stadig større affinitet mellem teknologi og den lovfæstede ret til eller den offentlige forventning om privatlivets fred i forbindelse med indsamling og udveksling af data. Problemer med beskyttelse af privatlivets fred findes overalt, hvor entydige identitetsdata for en person, eller personer, indsamles og opbevares i digital form eller på anden vis. Fejlagtig eller manglende kontrol med offentliggørelse kan give anledning til fortrolighedsproblemer. De mest udbredte datakilder, der berøres af databeskyttelsesproblematikken, er sundhedsvæsenet, det strafferetlige område, finans, genetik og lokalisering. Lokalisering er det vigtigste element i RFID.

4.5 I sin vejledning ([4]) til, hvordan man forholder sig til databeskyttelse og overholdelse af privatlivets fred, har Kommissionen fastlagt otte principper for god praksis. Den siger, at data skal:

— bearbejdes lovligt og på en rimelig måde

— bearbejdes til begrænsede formål

— være tilstrækkelige, relevante og ikke overdrevne

— være præcise

— ikke opbevares længere end nødvendigt

— bearbejdes i overensstemmelse med de registreredes rettigheder

— være sikre

— ikke videregives til andre lande uden tilstrækkelig beskyttelse.

Disse retningslinjer svarer fuldt ud til bestemmelserne om privatlivets fred og datasikkerhed i forbindelse med anvendelse af RFID.

([3]) http://cordis.europa.eu/fp7/dc/index.cfm?fuseaction=UserSite.CooperationDetailsCallPage&call_id=11.
([4]) Databeskyttelsesdirektiv 94/46/EØF, artikel 6.

4.6 Ifølge EØSU er de grundlæggende principper for god praksis følgende:

— RFID-brugere skal offentliggøre deres politikker og praksis, og der bør ikke findes hemmelige databaser med personoplysninger.

— Den enkelte har ret til at vide, hvornår varer i detailhandlen er udstyret med RFID-tags eller aflæsere. Enhver tag-aflæsning, der foregår i detailhandlen, bør foregå på gennemskuelig vis for alle parter.

— RFID-brugere skal oplyse om formålene med anvendelse af tags og aflæsere. Indsamling af oplysninger bør begrænses til, hvad der er nødvendigt for det pågældende formål.

— RFID-brugere bærer ansvaret for anvendelsen af teknologien og for, at sikkerhedslovgivningen og retningslinjerne overholdes. De bærer også ansvaret for systemets og databasernes sikkerhed og integritet.

4.7 Hvordan disse principper skal omsættes i praksis er et åbent spørgsmål. Ideelt set skulle enhver virksomhed, som indgår forretningsaftaler med kunder ved detailhandel, billetudstedelse, adgangskontrol eller transportydelser, udstede kunderne en form for garanti for, at principperne vil blive fulgt, en form for kundecharter. Et sådant charter kunne indeholde de principper for god praksis vedrørende databeskyttelse, som beskrives i punkt 4.5. Desuden foreslår EØSU følgende retningslinjer:

a) Det bør være forbudt for de handlende at presse eller tvinge kunderne til at acceptere aktive eller passive tags i de produkter, de køber. En mulighed kunne være, at tags placeres på emballagen eller at man anvender tags, der kan fjernes på samme måde som prismærker.

b) Kunderne skal frit kunne fjerne eller desaktivere tags, der er placeret på genstande i deres besiddelse.

c) RFID bør, som hovedregel, ikke anvendes til at spore personer. Sporing af mennesker er upassende, uanset om det sker gennem f.eks. tøj, varer, billetter eller andre ting.

d) RFID bør aldrig anvendes med henblik på at afskaffe eller indskrænke anonymitet.

e) Den ansvarlige myndighed bør give klare instrukser om, at (c) og (d) kun kan tillades under særlige omstændigheder og efter forudgående formel underretning af myndigheden.

4.8 Enkelte undtagelser fra ovenstående retningslinjer kan komme på tale, når:

— enkeltpersoner i egen interesse vælger at bibeholde aktive tags;

— enkeltpersoner indvilliger i at blive sporet i kritiske omgivelser, som f.eks. sikrede private og offentlige anstalter og institutioner;

— enkeltpersoner vælger at benytte applikationer, som lokaliserer og identificerer dem på samme måde som de allerede nu lokaliseres og identificeres ved brug af mobiltelefoner, betalingskort, internetadresser osv.

Enhver af disse undtagelser skal oplyses til den ansvarlige myndighed.

4.9 En gruppe af systemanvendelser, som kunne fritages, er sporing af mennesker eller varer i kortere perioder og under særlige forhold. Inden for luftfarten kunne bagage udstyres med tags ved check-in, så man forbedrer sikkerheden og visheden for håndtering af bagage, mens passagerer kunne udstyres med tags, så man bedre og rettidigt kunne afvikle flyafgange og hurtigere kunne gennemføre sikkerhedsprocessen. En anden systemanvendelse kunne være sporing af patienter efter hospitalsindlæggelse i forbindelse med operation. Nøglen til accept af denne form for anvendelse kan være visheden om, at taggen desaktiveres ved afslutningen på det kortvarige ophold.

4.10 RFID er ingen færdigudviklet teknologi, så vi kender endnu ikke dens fulde potentiale. På den ene side indebærer den måske ufattelige fordele for vores teknologiske civilisation, på den anden side er det måske vor tids største teknologiske trussel mod privatlivets fred og friheden. EØSU er af den overbevisning, at RFID-systemanvendelser bør udvikles i overensstemmelse med strenge etiske regler om privatlivets fred, frihed og datasikkerhed, men systemudviklingen bør fortsætte under forudsætning af, at de nødvendige forholdsregler træffes.

4.11 Kort sagt bør implementeringen være fuldt ud gennemskuelig for alle involverede parter, når RFID-applikationer er tilladte. Generelt er systemanvendelser, der letter håndteringen af varer, acceptabel. Systemanvendelser, der medfører, at mennesker udstyres med tags, kan som hovedregel kun accepteres i kortere perioder. Systemanvendelser, som forbinder mennesker til varer, kan accepteres med henblik på markedsføring. RFID-anvendelser, som identificerer mennesker gennem varer, de har købt, er som hovedregel uacceptable. Derudover passer visse systemanvendelser slet ikke ind i et frit samfund og bør derfor aldrig tillades. Det centrale i Kommissionens henstilling til medlemsstaterne må være det bydende behov for at værne om privatlivets fred og anonymiteten.

Bruxelles, den 11. juli 2007

Dimitris DIMITRIADIS

Formand for

Det Europæiske Økonomiske og Sociale Udvalg