I

(Beslutninger og resolutioner, henstillinger og udtalelser)

UDTALELSER

DEN EUROPÆISKE TILSYNSFØRENDE FOR DATABESKYTTELSE

Udtalelse fra Den Europæiske Tilsynsførende for Databeskyttelse om meddelelsen fra Kommissionen til Europa-Parlamentet, Rådet, Det Europæiske Økonomiske og Sociale Udvalg og Regionsudvalget om radiofrekvensbaseret identifikation (RFID) i Europa: elementer til en politisk ramme KOM(2007) 96

(2008/C 101/01)

DEN EUROPÆISKE TILSYNSFØRENDE FOR DATABESKYTTELSE,

som henviser til traktaten om oprettelse af Det Europæiske Fællesskab, særlig artikel 286,

som henviser til Den Europæiske Unions charter om grundlæggende rettigheder, særlig artikel 8,

som henviser til Europa-Parlamentets og Rådets direktiv 95/46/EF af 24. oktober 1995 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger,

som henviser til Europa-Parlamentets og Rådets direktiv 2002/58/EF af 12. juli 2002 om behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor,

som henviser til Europa-Parlamentets og Rådets forordning (EF) nr. 45/2001 af 18. december 2000 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger i fællesskabsinstitutionerne og -organerne og om fri udveksling af sådanne oplysninger, særlig artikel 41,

HAR VEDTAGET FØLGENDE UDTALELSE:

I. INDLEDNING

1. Kommissionen vedtog den 15. marts 2007 en meddelelse om radiofrekvensbaseret identifikation (RFID) i Europa: elementer til en politisk ramme [1] (i det følgende benævnt »meddelelsen«). I henhold til artikel 41 i forordning (EF) nr. 45/2001 har den tilsynsførende til opgave at rådgive fællesskabsinstitutioner og fællesskabsorganer om og spørgsmål vedrørende behandling af personoplysninger. I overensstemmelse med denne artikel forelægger den tilsynsførende hermed denne udtalelse.

2. Denne udtalelse skal ses som den tilsynsførendes reaktion på meddelelsen samt på andre foranstaltninger på RFID-området, der er truffet siden meddelelsens vedtagelse. Disse andre relevante foranstaltninger, som er taget i betragtning i denne udtalelse, er:

— Kommissionens afgørelse af 28. juni 2007 om nedsættelse af ekspertgruppen om radiofrekvensidentifikation [2], en direkte konsekvens af meddelelsen. Denne gruppe kendes også som gruppen af RFID-interessenter. I henhold til artikel 4, stk. 4, litra b), i afgørelsen deltager den tilsynsførende i gruppens aktiviteter som observatør.

— Rådets resolution af 22. marts 2007 om en strategi for et sikkert informationssamfund i Europa [3].

— Projektet RFID og identitetsstyring, som Europa-Parlamentet har taget initiativ til [4].

[1] KOM(2007) 96 endelig.
[2] Afgørelse 467/2007/EF (EUT L 176 af 6.7.2007, s. 25).
[3] EUT C 68 af 24.3.2007, s. 1.
[4] Projektet »RFID and identity management — Case studies from the frontline of the development towards ambient intelligence«, som er bestilt af Europa-Parlamentets tjeneste for vurdering af videnskabelige og teknologiske projekter (STOA) og gennemført af ETAG (European Technology Assessment Group) http://www.europarl.europa.eu/stoa/default_en.htm

— Artikel 29-Databeskyttelsesgruppens vedtagelse i juni 2007 af udtalelse nr. 4/2007 om begrebet personoplysninger ([1]).

— Meddelelsen fra Kommissionen til Europa-Parlamentet og Rådet om opfølgning på arbejdsprogrammet for en bedre gennemførelse af databeskyttelsesdirektivet ([2]) og den tilsynsførendes udtalelse om denne meddelelse af 25. juli 2007 ([3]).

— Kommissionens vedtagelse af et forslag til direktiv om ændring af bl.a. direktiv 2002/58/EF om behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor ([4]).

3. Den tilsynsførende hilser Kommissionens meddelelse om RFID velkommen, da den behandler de vigtigste spørgsmål i forbindelse med ibrugtagning af RFID-teknologi uden at se bort fra de afgørende spørgsmål vedrørende privatlivets fred og databeskyttelse. Det forberedende arbejde har været grundigt og gennemført. Fem tematiske seminarer samt en offentlig onlinehøring ([5]), der var bestilt af Kommissionen, er således gået forud for meddelelsen.

4. Den tilsynsførende tilslutter sig det synspunkt, at RFID-systemer vil kunne spille en vigtig rolle i forbindelse med udviklingen af informationssamfundet, der normalt omtales som »tingenes internet«, og han deler også fuldt ud de betænkeligheder, der er nævnt i punkt 3.2 i meddelelsen, nemlig at RFID-systemer vil kunne true privatlivets fred og databeskyttelsesrettighederne. Den tilsynsførende pegede i sin årsberetning 2005 på RFID sammen med biometri, intelligente omgivelser og identitetsstyringssystemer som teknologiske udviklinger, der forventes at få stor betydning for databeskyttelsen.

5. Ifølge den tilsynsførende vil beherskelsen af RFID-teknologier og den udbredte accept af dem ikke alene blive opnået i kraft af deres bekvemme brugervenlighed eller de nye tjenester, de fører med sig, men vil også blive lettet i kraft af de fordele, der er ved skræddersyede og konsekvente databeskyttelsesgarantier.

6. Kort sagt: Den tilsynsførende betegner RFID som en grundlæggende ny teknologisk udvikling, der i Kommissionens meddelelse med rette omtales som nøglen til en ny fase i informationssamfundets udvikling.

7. Denne udvikling rejser vigtige spørgsmål på forskellige områder, herunder området for databeskyttelse og privatlivets fred. Den tilsynsførendes udtalelse er begrænset til dette område.

II. UDTALELSENS FOKUS

8. Udtalelsen er især fokuseret på denne udviklings eventuelle konsekvenser for databeskyttelsen og privatlivets fred. Disse konsekvenser er for øjeblikket usikre, også fordi udviklingen af RFID-systemer og beherskelsen heraf er i fuld gang, og at det på ingen måde står klart, hvor udviklingen vil ende.

9. Under hensyn hertil anlægger den tilsynsførende følgende tilgang:

— For det første er det nødvendigt at afdække de praktiske konsekvenser af ibrugtagningen af RFID-systemerne for databeskyttelsen og privatlivets fred.

— For det andet er det nødvendigt at præcisere disse konsekvenser for databeskyttelsen og privatlivets fred i relation til den nuværende retlige ramme.

— For det tredje ser den tilsynsførende nærmere på, om disse konsekvenser kræver mere specifikke regler til imødegåelse af de databeskyttelsesspørgsmål, der opstår ved anvendelse af RFID-teknologier. Den tilsynsførende tog allerede dette spørgsmål op i sin udtalelse om meddelelsen om databeskyttelsesdirektivet og det vil blive yderligere uddybet i denne udtalelse.

10. Med denne tilgang søger den tilsynsførende at medvirke til, at udviklingen af RFID-systemer og beherskelsen heraf skal tilgodese berettigede bekymringer med hensyn til databeskyttelse og privatlivets fred.

III. AFDÆKNING AF KONSEKVENSERNE

RFID-systemer og -etiketter

11. Selv om udviklingen som nævnt er i fuld gang, og resultatet er usikkert, er det alligevel muligt at beskrive de vigtigste kendetegn ved udviklingen med henblik på dens konsekvenser for databeskyttelsen.

([1]) Dok. WP 136, der er offentliggjort på gruppens websted.
([2]) Meddelelse af 7. marts 2007 fra Kommissionen til Europa-Parlamentet og Rådet om opfølgning på arbejdsprogrammet for en bedre gennemførelse af databeskyttelsesdirektivet, KOM(2007) 87 endelig.
([3]) EUT C 255 af 27.10.2007, s. 1. I det følgende benævnt: »Udtalelsen om meddelelsen om databeskyttelsesdirektivet«.
([4]) Forslag af 13. november 2007 til Europa-Parlamentets og Rådets direktiv om ændring af direktiv 2002/22/EF om forsyningspligt og brugerrettigheder i forbindelse med elektroniske kommunikationsnet og -tjenester, Europa-Parlamentets og Rådets direktiv 2002/58/EF af 12. juli 2002 om behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor og forordning (EF) nr. 2006/2004 om forbrugerbeskyttelsessamarbejde, KOM(2007) 698 endelig. Direktivet 2002/58/EF vil blive omtalt som »e-databeskyttelsesdirektivet«.
([5]) http://www.rfidconsultation.eu/

12. Ved vurderingen af de potentielle aspekter af RFID-teknologien, der har indvirkning på databeskyttelsen og privatlivets fred, er det særdeles relevant ikke blot af se på RFID-etiketterne, men på hele RFID-infrastrukturen: etiketten, læseapparatet, nettet, referencedatabasen og den database, hvor de oplysninger, der produceres i samspillet mellem etiket og læseapparat, er lagret. Som det kort understreges i indledningen til meddelelsen, er RFID ikke bare »elektroniske mærkater«, og databeskyttelsesspørgsmålene vil derfor ikke være begrænset til etiketter alene, men udstrække sig til alle dele af den overordnede RFID-infrastruktur. Hvert enkelt af disse elementer har således en rolle at spille ved at bidrage til gennemførelsen af den europæiske retlige ramme for databeskyttelse, når det er nødvendigt. De vil blive stimuleret af hovedtendenserne i det informationssamfund, der er under udvikling, som f.eks. en næsten ubegrænset båndvidde, allestedsnærværende netforbindelser og uendelig lagringskapacitet.

RFID-systemers og -etiketters virkning

13. Uanset behovet for en bredere tilgang som understreget i det foregående punkt er der forskellige grunde til først at fokusere på anvendelsen af RFID til mærkning af individuelle genstande som f.eks. forbrugsvarer i detailsektoren. Den mest indlysende grund er den øgede brug der forventes, og som synes at bevæge sig i retning af en vidt udbredt anvendelse. I modsætning til andre RFID-anvendelser med snæver eller begrænset anvendelse har mærkning af individuelle genstande potentiale til at blive en massemarkedsanvendelse. Mange forbrugsvarer er allerede nu udstyret med en RFID-etiket. Med hertil hører, at denne anvendelse vil berøre et enormt antal mennesker, hvis personoplysninger vil kunne blive behandlet, hver gang de køber et produkt, hvori der er indbygget en RFID-etiket.

14. Man bør være særlig opmærksom på konsekvenserne af RFID-mærkning for ejerne af genstande. RFID-systemer vil kunne etablere en forbindelse mellem en genstand og dens ejer. Når denne forbindelse først er etableret, kan ejeren scannes og klassificeres som »lavbudget« eller »attraktivt mål« for fremtidige transaktioner; overdreven etablering af en-til-en-relationer ([1]) vil kunne medføre automatisk »straf« af visse former for adfærd (genvindingspligt, affald, osv.). Enkeltpersoner bør ikke være underlagt negative automatiserede beslutningsprocesser. Denne RFID-egenskab kan øge risikoen for, at informationssamfundet bevæger sig nærmere en situation, hvor der træffes automatiserede beslutninger, og hvor teknologi bliver misbrugt til at regulere menneskers adfærd.

15. De oplysninger, der er lagret i eller produceret af en RFID-etiket, kan være personoplysninger som defineret i artikel 2 i databeskyttelsesdirektivet. For eksempel kan chipkort, der anvendes i forbindelse med rejser, både indeholde identifikationsoplysninger og oplysninger om indehaverens seneste rejser. Hvis en skrupelløs person ønsker at spore personer, vil det være tilstrækkeligt at placere læseapparater på strategiske steder, så de giver oplysninger om kortindehaveres bevægelser, hvilket vil være en krænkelse af privatlivets fred og en overtrædelse af reglerne om personoplysninger.

16. Tilsvarende trusler mod privatlivets fred kan opstå, selv om de oplysninger, der er lagret i RFID-etiketten, ikke omfatter navne på enkeltpersoner. RFID-etiketter indeholder unikke identifikatorer, der er knyttet til forbrugsvarer: hvis hver etiket har en unik identifikator, kan denne identifikation anvendes til overvågningsformål. Hvis for eksempel en person bærer et armbåndsur, som har en RFID-etiket, der indeholder et id-nummer, kan dette også anvendes som en unik identifikator for bæreren af uret, selv om hans identitet ikke kendes. Alt efter den måde, oplysningerne anvendes på — og sættes i relation til selve uret eller personen-, kan direktivet finde anvendelse eller ikke. Det vil f.eks. finde anvendelse, hvis der fremkommer oplysninger om personers opholdssted, som vil kunne anvendes til at overvåge deres adfærd eller for eksempel med henblik på prisdifferentiering, nægtelse af adgang eller uønsket udsættelse for reklame.

17. Det er i denne forbindelse nødvendigt at sikre, at RFID-anvendelser tages i brug med de nødvendige teknologiske forholdsregler for at minimere risikoen for utilsigtet videregivelse af oplysninger. Sådanne forholdsregler kan omfatte kravet om, at RFID-infrastrukturen, især RFID-etiketter, designes på en måde, der hindrer et sådant resultat. RFID-etiketter kan f.eks. forsynes med en »kill command«, der gør det muligt at deaktivere dem. Denne mulighed vil blive drøftet yderligere i kapitel IV i denne udtalelse.

18. Ved at gøre det muligt at spore varer ud over salgsstedet indfører RFID-systemer nye spørgsmål i debatten om privatlivets fred. Der er således to elementer, som skal tages i betragtning i analysen af virkningen: hvor personlig genstanden anses for at være, og genstandens mobilitet ([2]).

19. En genstands levetid vil også kunne indgå i den krævede risikoanalyse og bidrage til den kvantitative vurdering af de potentielle trusler mod privatlivets fred. Forudsat at en etiket ikke deaktiveres, vil et slutbrugerprodukt med en lang levetid kunne samle flere oplysninger om ejeren af produktet og opbygge en mere nøjagtig profil. Omvendt kan en kort levetid for en genstand som f.eks. en dåse sodavand fra produktion til genvinding udgøre færre risici og derfor kræve lempeligere forholdsregler end et produkt med en meget længere levetid.

([1]) Dr. Sarah Spiekermann, director Berlin Research Centre on Internet Economics, workshop on RFID and ubiquitous computing organized by the Trans Atlantic Consumer Dialogue, 13 March 2007.

([2]) Dara J. Glasser, Kenneth W. Goodman and Norman G. Einspruch, Chips, tags and scanners: Ethical challenges for radio frequency identification, Ethics and Information Technology, Volume 9, No. 2/2007.

Spørgsmål vedrørende privatlivets fred og databeskyttelse i forbindelse med ibrugtagningen af RFID-systemer

20. For bedre at forstå RFID-systemernes konsekvenser for privatlivets fred og databeskyttelsen kan der sondres mellem fem grundlæggende spørgsmål vedrørende sikkerheds- og privatlivsbeskyttelse.

21. Det første spørgsmål er identifikationen af den registrerede. For over tres år siden var formålet med RFID-etiketten at »identificere den ven eller fjende«, der var på vej. I dag kan RFID-systemerne ikke blot identificere generelle elementer ved en genstand, men kan også i sidste ende føre til identifikation af en person og må derfor gøre det på en databeskyttelsesvenlig måde.

22. Det andet spørgsmål er identifikationen af den/de registeransvarlige. I forbindelse med RFID-systemer kan identifikationen af den registeransvarlige som defineret i artikel 2, litra d), i databeskyttelsesdirektivet være vanskeligere at foretage og skal derfor undersøges nøjere. Identifikationen af den registeransvarlige er imidlertid fortsat et kritisk skridt i fastlæggelsen af ansvaret for hver enkelt af de relevante aktører, der skal overholde den retlige ramme for databeskyttelsen. I løbet af etikettens levetid kan den registeransvarlige, som behandler oplysningerne, skifte flere gange på grundlag af de yderligere tjenester, der kan leveres i forbindelse med den mærkede genstand.

23. Det tredje spørgsmål er den reducerede betydning af den traditionelle sondring mellem den personlige og den offentlige sfære. Selv om sondringen mellem det private og det offentlige rum heller ikke tidligere altid har været skarp, er de fleste bevidst om grænserne mellem dem (og om de grå zoner) og træffer i overensstemmelse hermed informerede eller intuitive beslutninger om, hvordan de skal handle. Ifølge Hall ([1]) giver personligt rum sig normalt udslag i fysisk afstand fra andre. Håndteringen af privatlivets fred kan også betragtes som en dynamisk grænsereguleringsproces ([2]). Det er derfor ikke overraskende, at det forhold, at etiketkommunikationen foregår trådløst og kan aflæses uden for synsvidde, giver anledning til bekymringer med hensyn til privatlivets fred, da den udvisker disse traditionelle grænser og håndteringen af dem. Der er faktisk frygt for, at den enkelte kan miste en del af eller al den kontrol med styringen af afstanden, som vedkommende hidtil har haft. Derfor har både fortalere og modstandere af RFID-systemerne fokuseret på læserækkevidden af de første systemer, der er blevet implementeret.

24. Det fjerde spørgsmål vedrører RFID-etiketters størrelse og fysiske egenskaber. Fordi etiketten først og fremmest skal være lille og billig, vil de sikkerhedsforanstaltninger, som kan træffes for denne del af RFID-systemet, pr. definition være begrænsede. Det forhold, at kommunikationen foregår trådløst, indebærer imidlertid også risici sammenlignet med trådkommunikation, og der er derfor behov for yderligere sikkerhedskrav.

25. Det femte spørgsmål er behandlingens manglende gennemsigtighed. RFID-systemer vil kunne føre til ubemærket indsamling og behandling af oplysninger, som kan anvendes til at udarbejde personprofiler. Denne konsekvens kan udmærket illustreres ved at sammenligne RFID-systemer med mobiltelefoner, en sammenligning, der ofte foretages. På den ene side har der været en meget høj grad af teknologisk accept af mobiltelefoner uanset de potentielle risici for krænkelse af privatlivets fred. Det kan antages, at RFID vil blive accepteret på samme måde. På den anden side må det understreges, at en mobiltelefon er en synlig genstand, som slutbrugeren bevarer kontrollen over, da den kan slukkes. Dette er ikke tilfældet med RFID.

26. Selv om ubemærket indsamling og behandling af oplysninger som nævnt ovenfor kan være legitim, er det også muligt og under forskellige omstændigheder endog ganske sandsynligt, at der forekommer uretmæssig indsamling og behandling af sådanne oplysninger.

27. Der kan på grundlag af dette kapitel drages følgende konklusion. Den omfattende brug af RFID-teknologi er grundlæggende ny og kan få dybtgående indvirkning på vort samfund og på beskyttelsen af de grundlæggende rettigheder i vort samfund som f.eks. privatlivets fred og databeskyttelse. RFID kan medføre en kvalitativ ændring.

IV. PRÆCISERING AF KONSEKVENSERNE

Indledning

28. Dette kapitel vil hovedsagelig fokusere på RFID'S indvirkning på beskyttelsen af de grundlæggende rettigheder i vort samfund som f.eks. privatlivets fred og databeskyttelsen. Dette vil blive nærmere præciseret i to tempi, hvor der først gives en kort beskrivelse af, hvordan disse grundlæggende rettigheder beskyttes i den nuværende retlige ramme. Dernæst vil den tilsynsførende uddybe mulighederne for at udnytte den nuværende retlige ramme fuldt ud. Dette ønske blev indsat i udtalelsen om meddelelsen om databeskyttelsesdirektivet som »direktivets nuværende bestemmelser skal være gennemført fuldt ud«.

29. Udgangspunktet er følgende: nye teknologiske udviklinger som f.eks. RFID-systemer har stor betydning for kravene til en effektiv retlig ramme for databeskyttelse. Desuden kan behovet for effektiv beskyttelse af det enkelte menneskes personoplysninger sætte begrænsninger for anvendelsen af de nye teknologier. Samspillet er derfor tosidet: teknologien påvirker lovgivningen, og lovgivningen påvirker teknologien ([3]).

([1]) Hall, E.T., 1966, The Hidden Dimension (1st ed.). Garden City, N.Y: Doubleday.

([2]) Altman, I., 1975, The Environment and Social Behaviour, Brooks/Cole Monterrey.

([3]) Jf. den tilsynsførendes bemærkninger fra marts 2006 om Kommissionens meddelelse om kompatibilitet mellem europæiske databaser, der er offentliggjort på den tilsynsførendes websted.

Beskyttelse af de grundlæggende rettigheder

30. Beskyttelsen af de grundlæggende rettigheder i forbindelse med privatlivets fred og databeskyttelse i Den Europæiske Union er for det første sikret ved en retlig ramme, hvilket er nødvendigt, da der er tale om rettigheder, som er anerkendt i artikel 8 i den europæiske konvention til beskyttelse af menneskerettigheder og grundlæggende frihedsrettigheder og i artikel 7 og 8 i Den Europæiske Unions charter om grundlæggende rettigheder. Den relevante lovgivningsmæssige ramme for databeskyttelse og RFID består først og fremmest af databeskyttelsesdirektivet 95/46/EF og e-databeskyttelsesdirektivet 2002/58/EF ([1]).

31. Den generelle lovgivningsmæssige ramme for databeskyttelse som fastlagt i direktiv 95/46/EF gælder for RFID, for så vidt oplysninger, som behandles af RFID-systemer, falder inden for definitionen af personoplysninger. Mens RFID-anvendelser i visse tilfælde klart behandler personoplysninger og utvivlsomt falder inden for databeskyttelsesdirektivets anvendelsesområde, er der også anvendelser, hvor det måske ikke er så åbenlyst, at databeskyttelsesdirektivet skal anvendes. Artikel 29-Databeskyttelsesgruppens om udtalelse nr. 4/2007 om begrebet personoplysninger tager sigte på at bidrage til en klarere og almindeligt anerkendt forståelse af begrebet personoplysninger og begrænser således denne usikkerhed ([2]).

32. For så vidt angår e-databeskyttelsesdirektivet er situationen følgende. Det har hidtil ikke været klart, om dette direktiv finder anvendelse på RFID-anvendelser. Derfor indeholder Kommissionens forslag af 13. november 2007 om ændring af direktivet en bestemmelse, der skal præcisere, at direktivet faktisk finder anvendelse på visse RFID-anvendelser. Andre RFID-anvendelser vil imidlertid måske ikke være omfattet, fordi dette direktiv er begrænset til behandling af personoplysninger i forbindelse med udbud af offentligt tilgængelige elektroniske kommunikationstjenester i offentlige kommunikationsnet.

33. Beskyttelsen af personoplysninger kan suppleres med en række selvregulerende instrumenter (ikke-lovgivningsmæssig ramme). Anvendelsen af disse instrumenter fremmes aktivt i begge direktiver, især i artikel 27 i databeskyttelsesdirektivet, som fastsætter, at medlemsstaterne og Kommissionen tilskynder til udarbejdelsen af adfærdskodekser, der (…) skal bidrage til en korrekt anvendelse af direktivet. Desuden kan selvregulerende instrumenter effektivt bidrage til gennemførelsen af de sikkerhedsforanstaltninger, der kræves i artikel 17 i databeskyttelsesdirektivet og artikel 14 i e-databeskyttelsesdirektivet.

([1]) I punkt 59 i denne udtalelse drøftes relevansen af et tredje direktiv, nemlig Europa-Parlamentets og Rådets direktiv 1999/5/EF af 9. marts 1999 om radio- og teleterminaludstyr samt gensidig anerkendelse af udstyrets overensstemmelse (EFT L 91 af 7.4.1999, s. 10).

([2]) Jf. bl.a. s. 10 i udtalelsen, som er nævnt i fodnote 5.

Fuld gennemførelse af den nuværende ramme

34. Udtalelsen om meddelelsen om databeskyttelsesdirektivet nævner en række redskaber, der er til rådighed med henblik på en bedre gennemførelse af direktivet. De fleste af de ikke-bindende redskaber i denne udtalelse er relevante for RFID som f.eks. fortolkningsmeddelelser eller andre meddelelser, fremme af bedste praksis, anvendelse af datasikkerhedsmærkning og eksterne databeskyttelsesaudits. Muligheden for at vedtage særlige regler for RFID vil blive drøftet i kapitel V. Men forbedringer er mulige, også inden for den nuværende ramme.

Selvregulerende instrumenter

35. Den tilsynsførende er enig med Kommissionen i, at det i en første fase er hensigtsmæssigt at give mulighed for selvregulering, således at interessenterne hurtigt kan skabe et miljø, der er i overensstemmelse med reglerne, og således bidrage til at skabe et mere sikkert retligt miljø.

36. Kommissionen forventes i samråd med gruppen af RFID-interessenter at fremme og styre denne selvreguleringsproces. I denne forbindelse hilser den tilsynsførende den henstilling, som nævnes i meddelelsen, og som forventes at indeholde særlige retningslinjer for, »hvilke principper myndighederne og andre berørte parter bør følge i forbindelse med brug af RFID«, velkommen.

37. Meddelelsen forudser, at selvregulering tager form af en adfærdskodeks eller en kodeks for god praksis. Ifølge den tilsynsførende bør selvregulering, uafhængigt af hvilken form den antager:

— Give konkret og praktisk vejledning om særlige typer RFID-anvendelser og således bidrage til at overholde den retlige ramme for databeskyttelsen.

— Behandle de særlige spørgsmål og problemer vedrørende databeskyttelse, som opstår i forbindelse med generiske RFID-anvendelser.

— Bidrage til en ensartet og harmoniseret anvendelse af databeskyttelsesdirektivet i hele EU netop i en sektor, som sandsynligvis vil gøre brug af samme type RFID-anvendelser i hele EU.

— Anvendes af alle relevante interessenter. Manglende overholdelse bør have negative (eventuelt finansielle) konsekvenser.

38. Den tilsynsførende peger på et spørgsmål, hvor selvregulering vil være specielt nyttigt. For så vidt angår de RFID-anvendelser, der indebærer behandling af personoplysninger, pålægger databeskyttelsesdirektivet de registeransvarlige forskellige forpligtelser, især i henhold til artikel 17 (behandlingssikkerhed) og artikel 7 (nødvendigheden af kun at behandle oplysninger ud fra et fyldestgørende juridisk grundlag). Ifølge disse bestemmelser skal de registeransvarlige på den ene side træffe foranstaltninger mod ubeføjet videregivelse af oplysningerne. På den anden side skal de registeransvarlige sikre, at behandlingen som f.eks. videregivelse af oplysninger gennem læseapparaterne, hvor det er relevant, kun sker med informeret samtykke fra den person, som oplysningerne vedrører.

39. Disse bestemmelser i databeskyttelsesdirektivet kan fortolkes således, at de kræver, at der sammen med RFID-anvendelser iværksættes de nødvendige tekniske løsninger for at hindre eller minimere risikoen for uønsket videregivelse og sikre, at behandling eller overførsel af oplysninger kun sker med informeret samtykke, hvor det er relevant. Efter den tilsynsførendes opfattelse vil eksistensen af en sådan forpligtelse (dvs. til at anvende de nødvendige tekniske løsninger for at hindre eller minimere risikoen for uønsket videregivelse) og den omstændighed, at den er bindende for dem, der iværksætter RFID-anvendelser, være endnu stærkere og klarere, hvis dette krav optages i ovennævnte kommende adfærdskodeks eller kodeks for god praksis. Af disse årsager vil den tilsynsførende stærkt tilråde, at Kommissionens henstilling indeholder en sådan fortolkning af databeskyttelsesdirektivet og understreger eksistensen af en pligt til sammen med RFID-anvendelser at iværksætte de nødvendige teknologiske løsninger for at hindre uønsket indsamling eller videregivelse af oplysninger.

Behovet for vejledning

40. Den tilsynsførende anbefaler, at Kommissionen i tæt samarbejde med RFID-ekspertgruppen udarbejder et eller flere dokumenter, der giver en klar vejledning i, hvordan den nuværende retlige ramme skal anvendes på RFID-miljøet. Vejledningen bør give praktiske anvisninger på, hvordan principperne i databeskyttelsesdirektivet og e-databeskyttelsesdirektivet overholdes. Hvad angår vejledningens tilgang som helhed og dens konkrete indhold har den tilsynsførende følgende forslag.

41. Vejledningen skal fastsætte de principper, der gælder for RFID-brug, og skal være tilstrækkelig målrettet og anlægge en sektorspecifik tilgang. En udifferentieret tilgang vil ikke opfylde formålene, der er at sikre en klar og sammenhængende ramme. I stedet skal vejledningens anvendelsesområde være begrænset til veldefinerede sektorspecifikke RFID-anvendelser.

42. Desuden skal retningslinjer foreslå praktiske og effektive metoder til udvikling af teknikker og standarder, der kan bidrage til, at RFID-systemerne overholder den retlige ramme for databeskyttelsen, og som indebærer brug af »privacy by design« (indbygget databeskyttelse)-teknologi.

43. Der skal ved anvendelsen af den nuværende retlige ramme på RFID-miljøet lægges særlig vægt på at anvende de databeskyttelsesprincipper og -forpligtelser, der gælder for registeransvarlige i forbindelse med RFID-anvendelser. Særlig relevante er følgende forpligtelser og principper:

— Princippet om retten til information, herunder retten til at vide, hvornår der indsamles data gennem læseapparater, og i relevante tilfælde at produkter er mærket.

— Begrebet samtykke som en del af det juridiske grundlag for at behandle oplysninger. Dette begreb konkretiseres i pligten til at deaktivere RFID-etiketter på salgsstedet, medmindre den registrerede har givet sit samtykke ([1]). Retten til at deaktivere RFID-etiketter tjener også det formål at sikre oplysningernes sikkerhed, dvs. at sikre, at oplysninger, der behandles gennem RFID-etiketter, ikke videregives til uønskede tredjeparter.

— Enkeltpersoners ret til ikke at være underlagt negative beslutninger, der udelukkende er baseret på automatiseret behandling af en defineret personprofil.

44. For så vidt angår retten til information bør vejledningen fastsætte, at enkeltpersoner skal have information om behandlingen af deres personoplysninger. De bør især gøres opmærksom på bl.a. i) forekomsten af læseapparater og af aktiverede RFID-etiketter på produkter eller disses emballage, ii) konsekvenserne heraf med hensyn til indsamling af oplysnnger, og iii) hvilke formål de indsamlede oplysninger skal anvendes til.

45. Anvendelsen af logoer kan være egnet som foranstaltning til at give information. Logoer kan anvendes til at gøre opmærksom på læseapparater og RFID-etiketter, som det er meningen skal forblive aktive. Anvendelsen af logoer alene vil dog ikke være tilstrækkeligt til at sikre en loyal behandling af oplysninger, som kræver, at de registrerede informeres på en klar og forståelig måde. Anvendelsen af logoer bør anses for en foranstaltning, der supplerer formidlingen af mere detaljeret information.

([1]) Jf. punkt 46-50 i denne udtalelse, der indeholder flere detaljer.

Grundpillen: Opt-in-princippet

46. For alle relevante RFID-anvendelser bør det være en forudsætning, at løsningerne respekterer og gennemfører opt-in-princippet på salgsstedet. Det bør være ulovligt at sætte RFID-etiketter i stand til at fortsætte med at fremsende oplysninger efter salgsstedet, medmindre den registeransvarlige har fyldestgørende juridiske grunde. Et fyldestgørende juridisk grundlag vil normalt kun være a) den registreredes samtykke eller b) hvis denne videregivelse er nødvendig for at levere en tjenesteydelse, en specifik og frit fremsat anmodning fra nævnte person ([1]). Begge juridiske grundlag vil så opfylde betingelserne for opt in.

47. I henhold til opt-in-princippet bør etiketter deaktiveres på salgsstedet, medmindre den person, som har købt det produkt, som etiketten er knyttet til, ønsker at lade den forblive aktiv. Ved at udøve retten til at lade den forblive aktiv giver personen sit samtykke til viderebehandling af sine oplysninger, f.eks. til overførsel af oplysningerne til læseapparatet ved personens næste besøg hos den registeransvarlige.

48. For at imødegå RFID-anvendelsernes stadig større diversitet og lette udviklingen af nye innovative forretningsmodeller understreger den tilsynsførende betydningen af en fleksibel tilgang. Der skal være mulighed for fleksibilitet i forbindelse med gennemførelsen af opt-in-princippet.

49. Der er mange muligheder for at gennemføre opt-in-princippet. Som et alternativ til fjernelse af etiketten kan det f.eks. overvejes, at etiketten blokeres, gøres midlertidigt ubrugbar eller efter en sikkerhedspolitisk model kaldet »resurrecting duckling model« ([2]) låses til en specifik bruger. For så vidt angår en etiket med kort levetid vil etikettens adresse, som viser vej til oplysninger, der er lagret i en database, også kunne slettes fra referencedatabasen, således at der undgås viderebehandling af yderligere oplysninger, der indsamles af etiketten.

50. Konklusionen er, at selv om den tilsynsførende mener, at opt-in-princippet på salgsstedet er en retlig forpligtelse, der allerede findes ifølge databeskyttelsesdirektivet i de fleste situationer, er der gode grunde til at specificere denne forpligtelse i selvreguleringsinstrumenter, også for at sikre, at princippet gennemføres på den mest hensigtsmæssige måde. Det er under alle omstændigheder nødvendigt med en specifik gennemførelse for de RFID-anvendelser, der falder uden for databeskyttelsesdirektivets anvendelsesområde.

Behovet for »privacy by design« (indbygget databeskyttelse)

51. For at minimere truslerne mod privatlivets fred og databeskyttelsen støtter Kommissionens meddelelse i punkt 3.2 på side 6 ideen om udarbejdelse af specifikationer og vedtagelse af konstruktionskriterier. Den tilsynsførende hilser denne tilgang velkommen. Vedtagelsen af specifikationer og konstruktionskriterier, også kaldet de bedste tilgængelige teknikker (BAT) vil effektivt bidrage til databeskyttelsesregulering og datasikkerhedskrav. Denne fastlæggelse af teknologiske og organisatoriske kriterier vil, hvis de revideres hyppigt, styrke den symbiose mellem beskyttelse af privatlivets fred og sikkerhedskrav, som Den Europæiske Union er i gang med at udvikle.

52. Den rette definition af BAT i forbindelse med privatlivs- og datasikkerhedsbeskyttelse for RFID-systemer vil også være afgørende for at opbygge et pålideligt miljø, som kan bidrage til en bred accept heraf blandt slutbrugerne, samt for den europæiske industris konkurrenceevne.

53. Processen med at udvælge BAT til RFID-systemer bør stimuleres af konsekvensanalyser vedrørende privatlivs- og datasikkerhedsbeskyttelse, som der fortsat skal gøres en indsats for at få udarbejdet. Den tilsynsførende mener, at Det Europæiske Agentur for Net- og Informationssikkerhed (ENISA) sammen med Europa-Kommissionens fælles forskningscentre i samarbejde med de relevante interessenter i industrien kan bidrage til fastlæggelsen af denne bedste praksis og udviklingen af sådanne metoder. Ved den nylige indledning af projektet »tekniske retningslinjer for RFID« har det tyske forbundskontor for informationssikkerhed (BSI) givet et godt illustrerende eksempel ([3]) på BAT, som nu bør udvikles på europæisk plan.

54. Standarder kan også spille en afgørende rolle i forbindelse med indførelsen af princippet om indbygget databeskyttelse. Kommissionen bør derfor bidrage til, at der under udviklingen af internationale RFID-standarder indføres foranstaltninger med henblik på beskyttelse af privatlivets fred og datasikkerhed. Artikel 29-gruppen illustrerer klart i sit arbejdsdokument ([4]) om RFID, at standarder vil kunne bidrage til udviklingen af RFID-systemer, der tilgodeses privatlivets fred.

([1]) I forbindelse med nogle RFID-anvendelser kan det være muligt at anvende andre grundlag som f.eks. artikel 7, litra f) (den registeransvarliges legitime interesser med forbehold af tilstrækkelige garantier).

([2]) Navnet på denne model, der er udviklet af Frank Stajano og Ross Anderson fra Cambridge universitetet, er inspireret af »hvordan en gås, der udklækkes, antager, at den første genstand, den ser bevæge sig, må være dens mor«.

([3]) http://www.bsi.bund.de/veranst/rfid/index.htm

([4]) Arbejdsdokument (WP 105) om databeskyttelsesspørgsmål vedrørende RFID-teknologi af 19. januar 2005.

55. Desuden hilser den tilsynsførende den holdning velkommen, som Kommissionen har indtaget med hensyn til forskning og udvikling af RFID-teknologier og behovet for at mindske risikoen for privatlivets fred. Princippet om indbygget databeskyttelse skal således indføres i det første stadium af udviklingen af teknologier, hvilket bedre vil medvirke til overholdelsen af den retlige ramme for databeskyttelsen. Den tilsynsførende vil som kort beskrevet i årsberetningen 2006 tilslutte sig denne indsats ved fra sag til sag at afgive udtalelser og yde rådgivning vedrørende projekter under syvende rammeprogram (2007-2013).

V. ER DET NØDVENDIGT MED SPECIFIKKE LOVGIVNINGSFORANSTALTNINGER?

56. Selvregulering er muligvis ikke nok med henblik på fuld gennemførelse af den nuværende ramme for databeskyttelse og privatlivets fred. Selv om selvreguleringen opfylder ovennævnte krav er det frivillig at anvende og manglende overholdelse kan ikke altid sanktioneres effektivt. Desuden kan det fortsat være nødvendigt med bindende lovgivningsforanstaltninger til sikring af beskyttelsen af enkeltpersoners ret til privatlivets fred og databeskyttelse. Dette er så meget mere nødvendigt i tilfælde af, at den selvregulerede tilgang ikke virker.

57. Et vigtigt spørgsmål er bestemmelsen af de juridiske instrumenter, der er nødvendige for at sikre, at der sammen med RFID-anvendelserne faktisk iværksættes de nødvendige tekniske løsninger for at hindre eller minimere risikoen for databeskyttelsen og privatlivets fred, og at de registeransvarlige træffer passende foranstaltninger til at overholde deres forpligtelser i henhold til de eksisterende retlige rammer. Dette rejser nogle yderligere spørgsmål:

— Er der behov for specifikke regler?

— Hvis ja, kan disse regler vedtages inden for den nuværende lovgivningsmæssige ramme, f.eks. ved at gøre brug af de eksisterende udvalgsprocedurer?

— Eller er det nødvendigt med et nyt lovgivningsmæssigt instrument for at sikre en effektiv brug af RFID-anvendelser med indbyggede privatlivsfremmende teknologier.

58. Dette kapitel vil behandle mulighederne for at udstede bindende lovgivningsforanstaltninger inden for den nuværende retlige ramme, mens kapitel VI, fordi det er et særskilt spørgsmål, vil drøfte behovet for et nyt lovgivningsmæssigt instrument.

59. Man bør først være særlig opmærksom på bestemmelserne i artikel 17 i direktiv 95/46/EF, artikel 14, stk. 3, i direktiv 2002/58/EF og artikel 3, stk. 3, litra c), i direktiv 1999/5/EF. Artikel 14, stk. 3, gør det muligt for medlemsstaterne at vedtage foranstaltninger for at sikre, at terminaludstyr fremstilles på en måde, der er forenelig med brugernes ret til at beskytte og kontrollere anvendelsen af deres personoplysninger i overensstemmelse med direktiv 1999/5/EF ([1]). Direktiv 1999/5/EF fastsætter i artikel 3, stk. 3, litra c), at Kommissionen — efter en udvalgsprocedure — kan træffe afgørelse om, at apparatur inden for visse udstyrsklasser eller af særlige typer skal konstrueres på en sådan måde, at det er i stand til at sikre, at personoplysninger om brugeren og abonnenten og disses privatliv beskyttes. Artikel 3, stk. 3, litra c), i direktiv 1999/5/EF har ikke hidtil været anvendt.

60. Disse bestemmelser giver lovgiver beføjelse til — på nationalt plan og på fællesskabsplan — at foreskrive, at der skal indgå privatlivs- og databeskyttelsesforanstaltninger i fremstillingen af RFID-systemer, et begreb, der kaldes »privacy by design« (indbygget databeskyttelse) ([2]). Der skal også anvendes de bedste tilgængelige teknikker.

61. For at gøre brugen af begrebet indbygget databeskyttelse obligatorisk anbefaler den tilsynsførende, at Kommissionen anvender mekanismen i artikel 3, stk. 3, litra c), i direktiv 1999/5/EF i samråd med RFID-ekspertgruppen.

62. For det andet er det muligt at præcisere, hvordan den nuværende lovgivningsmæssige ramme skal anvendes på RFID, ved ændringer i selve direktiverne. Kommissionen har som nævnt netop forelagt et forslag om ændring af e-databeskyttelsesdirektivet, der indeholder en ny bestemmelse med henblik herpå. Den tilsynsførende hilser denne første bekræftelse af, at direktivet finder anvendelse på RFID-anvendelser, velkommen. Den tilsynsførende vil behandle de særlige spørgsmål vedrørende forbindelsen mellem e-databeskyttelsesdirektivet og RFID i sin udtalelse om ændringsforslaget, som vil blive udsendt i begyndelsen af 2008.

63. Da Kommissionen ikke forudser nogen ændring af databeskyttelsesdirektivet i den nærmeste fremtid ([3]), er mulighederne for præcisering af anvendelsen af den nuværende lovgivningsmæssige ramme på RFID begrænsede.

VI. ER DER BEHOV FOR EN SPECIFIK RETLIG RAMME FOR RFID?

Kommissionens planer

64. Meddelelsen ([4]) understreger betydningen af indbygget datasikkerheds- og privatlivsbeskyttelse. Den kræver også inddragelse af alle berørte parter. De vigtigste resultater af Kommissionens aktiviteter vil være »en henstilling om, hvilke

([1]) Og i overensstemmelse med Rådets afgørelse 87/95/EØF af 22. december 1986 om standardisering inden for informationsteknologi og telekommunikation (EFT L 36 af 7.2.1987, s. 31).
([2]) Jf. kapitel IV.
([3]) Den tilsynsførende støtter denne tilgang, jf. punkt 64.
([4]) Se punkt 4.1 i meddelelsen.

principper myndighederne og andre berørte parter bør følge i forbindelse med brug af RFID«. Henstillingen vil formentlig blive vedtaget i foråret 2008. De lovgivningsmæssige ambitioner, der nævnes i meddelelsen, omfatter to trin. Kommissionen vil:

— Overveje hensigtsmæssige bestemmelser om RFID i det kommende forslag til ændring af e-databeskyttelsesdirektivet. Som tidligere nævnt foreslog Kommissionen i november 2007 en sådan ændring af e-databeskyttelsesdirektivet og bekræftede direktivets anvendelighed på RFID-anvendelser ([1]), men foreslog ikke at udvide e-databeskyttelsesdirektivets anvendelsesområde til private net.

— Vurdere behovet for yderligere lovgivning til værn for data- og privatlivsbeskyttelse.

65. I overensstemmelse med denne politik kan det forventes, at Kommissionen ikke overvejer — i hvert fald ikke på kort sigt — at foreslå ny specifik lovgivning til værn for data- og privatlivsbeskyttelse på RFID-området.

Parametre for lovgiver

66. Den tilsynsførende nævnte i sin udtalelse om meddelelsen om databeskyttelsesdirektivet nogle hovedtræk for lovgivningsmæssige aktiviteter i forbindelse med behandling af personoplysninger, der kan sammenfattes således:

— For det første bør de vigtigste principper for databeskyttelsen bevares: »Der er ikke brug for nye principper, hvorimod der er et klart behov for andre administrative ordninger, der på den ene side er effektive og relevante for et netværkssamfund, og som på den anden side minimerer de administrative udgifter« ([2]).

— For det andet bør der kun forelægges forslag til lovgivning, hvis der er ført tilstrækkeligt bevis for deres nødvendighed og proportionalitet. Derfor bør den generelle lovgivningsmæssige ramme for databeskyttelse ikke ændres på kort sigt.

— For det tredje kan ændringer i samfundsudviklingen føre til specifikke retlige rammer med henblik på at tilpasse principperne fra databeskyttelsesdirektivet til de spørgsmål, som specifikke teknologier såsom RFID giver anledning til. Det er klart, at også i denne forbindelse skal betingelserne om nødvendighed og proportionalitet opfyldes.

67. Som et næste skridt er det nyttigt at præsicere de forventninger, som lovgiveren står over for på RFID-området:

— Lovgivningen skal være fleksibel og give plads til innovation og teknologisk udvikling. Dette bør føre til lovgivning, der er tilstrækkelig teknologisk neutral.

— For det andet skal lovgivningen give retssikkerhed. Dette bør føre til lovgivning, der er tilstrækkelig specifik. De berørte parter skal vide nøjagtigt, hvordan deres adfærd reguleres.

— For det tredje skal lovgivningen effektivt beskytte alle involverede legitime interesser. Dette kræver under alle omstændigheder håndhævelse af lovgivningen og en klar definition af ansvarsområderne: hvilken part er ansvarlig for hvilken adfærd ([3])? Disse krav gør sig endnu stærkere gældende, når det handler om privatlivets fred og databeskyttelse, personers grundlæggende rettigheder i henhold til den europæiske konvention om menneskerettigheder og grundlæggende frihedsrettigheder og Den Europæiske Unions charter om grundlæggende rettigheder.

Den tilsynsførendes holdning

68. Efter den tilsynsførendes opfattelse er det klart, at ikke al teknologisk udvikling bør afføde reaktioner fra den europæiske lovgivers side. Den teknologiske udvikling kan gå hurtigt, mens vedtagelsen og ikrafttrædelsen af lovgivning tager tid og bør tage tid. Lovgivning bør være et resultat af en afvejning af alle interesser, der er på spil. Når der vælges et direktiv som instrument, er der behov for endnu mere tid, da direktiver skal gennemføres fuldt ud i medlemsstaternes retssystemer.

69. RFID er imidlertid ikke blot endnu en teknologisk udvikling, som det understreges i flere dele af denne udtalelse. I meddelelsen henvises til RFID som nøglen til en ny fase i informationssamfundets udvikling, en fase, der sommetider går under betegnelsen »tingenes internet«, og RFID-etiketter vil komme til at spille en central rolle i de såkaldte intelligente omgivelser. Disse omgivelser er også vigtige skridt i udviklingen af, hvad der ofte kaldes »overvågningssamfundet« ([4]). På baggrund heraf kan lovgivningsmæssige tiltag på RFID-området berettiges. RFID kan medføre en kvalitativ ændring.

([1]) Se forslag til ny artikel 3 i direktiv 2002/58/EF.
([2]) Punkt 24 i udtalelsen om meddelelsen om databeskyttelsesdirektivet.
([3]) Udtrykt med databeskyttelsesterminologi medfører dette identifikation af »den registeransvarlige«.
([4]) Dette budskab blev gentaget i en erklæring fra de europæiske databeskyttelsesmyndigheder, der blev vedtaget i London den 2. november 2006, og som er tilgængelig på den tilsynsførendes websted: http://www.edps.europa.eu/EDPSWEB/edps/lang/en/pid/51

70. I dette perspektiv anbefaler den tilsynsførende, at det overvejes at vedtage (et forslag til) fællesskabslovgivning, der fastsætter regler for de vigtigste spørgsmål vedrørende RFID-brug i relevante sektorer i tilfælde af, at den nuværende retlige ramme ikke skulle blive gennemført på rette vis. Efter ikrafttrædelsen må en sådan lovgivningsmæssig foranstaltning betragtes som en »*lex specialis*« i forhold til den generelle ramme for databeskyttelse.

71. Vedtagelsen af et sådant lovgivningsmæssigt instrument vil have følgende fordele:

— Instrumentet kan fastsætte substantielle parametre for selvreguleringsmekanismerne.

— Perspektivet om vedtagelse af et lovgivningsmæssigt instrument kan vise sig at være et effektivt incitament for parterne til at indføre selvreguleringsmekanismer, der giver præcis beskyttelse.

72. For at gøre det mere praktisk kan Kommissionen anmodes om at udarbejde et høringsdokument om fordele og ulemper ved specifik lovgivning og om de vigtigste elementer i en sådan lovgivning. Parterne kan selvfølgelig anmodes om at bidrage til denne høring. På samme måde kan Artikel 29-gruppen inddrages.

Muligheder

73. Lovgiveren kan fastsætte en skræddersyet retlig ramme, der består af en blanding af regulerende værktøjer, der præciserer og supplerer den nuværende retlige ramme. Denne skræddersyede retlige ramme bør bygge på de kendte databeskyttelsesprincipper og bør fokusere på fordelingen af ansvarsområderne og kontrolmekanismernes effektivitet.

74. En specifik grund til, at der er behov for en sådan skræddersyet lovgivning, hænger sammen med, at ikke alle RFID-anvendelser indebærer behandling af personoplysninger. Med andre ord, hvis RFID-anvendelser ikke indebærer behandling af personoplysninger, er parter, der medvirker til fremstilling og salg af produkter med RFID, ikke juridisk tvunget til at gennemføre teknologiske foranstaltninger, der kan forhindre aflytning eller opsætning af læsseapparater uden forudgående advarsel til de pågældende personer. Som det er påvist, kan sådanne RFID-anvendelser imidlertid også indebære trusler mod privatlivets fred som følge af eventuel overvågning af personer, og de kræver således samme type værn om privatlivets fred. Dette kan netop være tilfældet ved mærkning af individuelle forbrugsvarer inden salget. Kort sagt kan RFID-anvendelser, der ikke behandler personoplysninger, stadig true privatlivets fred ved at give mulighed for skjult overvågning og anvendelse af oplysninger til uacceptable formål.

75. Den tilsynsførende mener, at dette uheldige resultat bør undgås. Fordi den nuværende lovgivning delvis — i hvert fald for RFID-anvendelser, der ikke behandler personoplysninger — ikke imødegår denne trussel mod privatlivets fred, og under hensyn til manglerne ved sot law-løsningerne forekommer det nødvendigt at anvende obligatoriske lovgivningsmæssige foranstaltninger for at sikre et tilfredsstillende resultat.

76. Sådanne foranstaltninger bør under alle omstændigheder:

— Fastlægge opt-in-princippet på salgsstedet som en præcis og ubestridelig retlig forpligtelse, også for RFID-anvendelser, der ligger uden for databeskyttelsesdirektivets anvendelsesområde ([1]).

— Sikre, at der sammen med RFID-anvendelser obligatorisk iværksættes hensigtsmæssige tekniske løsninger eller indbygget databeskyttelse.

VII. **FORVALTNINGSSPØRGSMÅLET**

77. Selv om den »iboende grænseoverskridende« dimension ved RFID-systemerne i meddelelsen alene anskues inden for det indre marked, mener den tilsynsførende, at denne dimension skal tackles på et mere internationalt plan. I en forretning er RFID-systemer allerede »grænseoverskridende«, eftersom etikettens aktivitet måske ikke stopper ved salgsstedet. På det generelle plan bliver RFID-teknologierne også »grænseoverskridende«, når overførsel af personoplysninger til et tredjeland kan finde sted, når producenten af den mærkede genstand, der er en del af RFID-systemet, har hjemsted uden for Den Europæiske Union ([2]).

78. Ud fra et mere fremtidsrettet synspunkt udgør forvaltningen af referencedatabaser med RFID-identiteter også en kritisk dimension for den rette håndhævelse af den europæiske retlige ramme for databeskyttelse. Den tilsynsførende tilskynder til, at der findes en løsning, da yderligere udhuling af denne ramme ikke vil være acceptabel.

79. Den tilsynsførende forudser, at spørgsmålet om RFID-forvaltning vil blive en større udfordring, der vil kræve betydelige investeringer. Det rette forhandlingsforum samt den mest hensigtsmæssige forvaltningsinfrastruktur skal findes for at sikre, at databeskyttelsesrettighederne respekteres på passende vis i disse internationale omgivelser.

([1]) I kapitel IV anføres det, at opt-in-princippet på salgsstedet er en retlig forpligtelse, der allerede findes ifølge databeskyttelsesdirektivet.

([2]) De forpligtelser, der gælder i forbindelse med videregivelse af personoplysninger, behandles i artikel 25 og 26 i databeskyttelsesdirektivet.

80. I dette perspektiv opfordrer den tilsynsførende Kommissionen til at fremlægge sine synspunkter vedrørende spørgsmålet om forvaltning, eventuelt i samråd med gruppen af RFID-interessenter.

VIII. **KONKLUSION**

81. Den tilsynsførende hilser Kommissionens meddelelse om RFID velkommen, da den behandler de vigtigste spørgsmål i forbindelse med ibrugtagning af RFID-teknologi uden at se bort fra de afgørende spørgsmål vedrørende privatlivets fred og databeskyttelse. Han deler det synspunkt, at RFID-systemer vil kunne spille en vigtig rolle i forbindelse med udviklingen af informationssamfundet, der normalt omtales som »tingenes internet«.

Afdækning af konsekvenserne

82. Den omfattende brug af RFID-teknologi er grundlæggende ny og kan få dybtgående indvirkning på vort samfund og på beskyttelsen af de grundlæggende rettigheder i vort samfund som f.eks. privatlivets fred og databeskyttelse. RFID kan medføre en kvalitativ ændring.

83. Der kan sondres mellem fem grundlæggende spørgsmål vedrørende datasikkerheds- og privatlivsbeskyttelse:

— Identifikationen af den registrerede.

— Identifikationen af den/de registeransvarlige.

— Den reducerede betydning af den traditionelle sondring mellem den personlige og den offentlige sfære.

— Konsekvenserne af RFID-etiketters størrelse og fysiske egenskaber.

— Behandlingens manglende gennemsigtighed.

Præcisering af konsekvenserne

84. Den generelle lovgivningsmæssige ramme for databeskyttelse som fastlagt i direktiv 95/46/EF gælder for RFID, for så vidt oplysninger, som behandles af RFID-systemer, falder inden for definitionen af personoplysninger.

85. For så vidt angår e-databeskyttelsesdirektivet: Kommissionens forslag af 13. november 2007 om ændring af direktivet indeholder en bestemmelse, der skal præcisere, at direktivet faktisk finder anvendelse på RFID-anvendelser. Andre RFID-anvendelser vil imidlertid måske ikke være omfattet, fordi dette direktiv er begrænset til behandling af personoplysninger i forbindelse med udbud af offentligt tilgængelige elektroniske kommunikationstjenester i offentlige kommunikationsnet.

86. Beskyttelsen af personoplysninger kan suppleres med en række selvregulerende instrumenter. Det er hensigtsmæssigt at give mulighed for selvregulering, forudsat at denne:

— Giver konkret og praktisk vejledning om særlige typer RFID-anvendelser.

— Behandler de særlige spørgsmål og problemer vedrørende databeskyttelse, som opstår i forbindelse med generiske RFID-anvendelser.

— Bidrager til en ensartet og harmoniseret anvendelse af databeskyttelsesdirektivet i hele EU.

— Anvendes af alle relevante interessenter.

87. Den tilsynsførende anbefaler, at Kommissionen i tæt samarbejde med RFID-ekspertgruppen udarbejder et eller flere dokumenter, der giver en klar vejledning i, hvordan den nuværende retlige ramme skal anvendes på RFID-miljøet.

88. Vejledningen skal fastsætte de principper, der gælder for RFID-brug, og skal være tilstrækkelig målrettet og anlægge en sektorspecifik tilgang. Den skal foreslå praktiske og effektive metoder til udvikling af teknikker og standarder, der kan bidrage til, at RFID-systemerne overholder den retlige ramme for databeskyttelsen, og som indebærer brug af »privacy by design« (indbygget databeskyttelse)-teknologi.

89. Den tilsynsførende ser med tilfredshed på tilgangen i Kommissionens meddelelse om at støtte ideen om udarbejdelse af specifikationer og vedtagelse af konstruktionskriterier.

90. Selv om den tilsynsførende mener, at opt-in-princippet på salgsstedet er en retlig forpligtelse, der allerede findes ifølge databeskyttelsesdirektivet i de fleste situationer, bør denne forpligtelse præciseres i selvreguleringsinstrumenter.

Er der behov for specifikke foranstaltninger?

91. For at gøre brugen af begrebet indbygget databeskyttelse obligatorisk anbefaler den tilsynsførende, at Kommissionen anvender mekanismen i artikel 3, stk. 3, litra c), i direktiv 1999/5/EF i samråd med RFID-ekspertgruppen.

92. Den tilsynsførende anbefaler, at det overvejes at vedtage (et forslag til) fællesskabslovgivning, der fastsætter regler for de vigtigste spørgsmål vedrørende RFID-brug i relevante sektorer i tilfælde af, at den nuværende retlige ramme ikke skulle blive gennemført på rette vis. Efter ikrafttrædelsen må en sådan lovgivningsmæssig foranstaltning betragtes som en »*lex specialis*« i forhold til den generelle ramme for databeskyttelse. Denne lovgivningsmæssige foranstaltning bør også tage fat på de spørgsmål med hensyn til privatlivs- og datasikkerhedsbeskyttelse, der opstår i forbindelse med visse RFID-anvendelser som f.eks. mærkning af individuelle genstande inden salget, som ikke nødvendigvis indebærer behandling af personoplysninger.

93. Kommissionen bør udarbejde et høringsdokument om fordele og ulemper ved specifik lovgivning og om de vigtigste elementer i en sådan lovgivning.

94. Lovgiveren kan fastsætte en skræddersyet retlig ramme, der består af en blanding af regulerende værktøjer, der præciserer og supplerer den nuværende retlige ramme. Foranstaltninger bør under alle omstændigheder:

— Fastlægge opt-in-princippet på salgsstedet som en præcis og ubestridelig retlig forpligtelse, også for RFID-anvendelser, der ligger uden for databeskyttelsesdirektivets anvendelsesområde ([1]).

— Sikre, at der sammen med RFID-anvendelser obligatorisk iværksættes hensigtsmæssige tekniske løsninger eller indbygget databeskyttelse.

Forvaltningsspørgsmålet

95. Den tilsynsførende opfordrer Kommissionen til at fremlægge sine synspunkter vedrørende spørgsmålet om forvaltning, eventuelt i samråd med gruppen af RFID-interessenter.

Udfærdiget i Bruxelles, den 20. december 2007.

Peter HUSTINX

Den Europæiske Tilsynsførende for Databeskyttelse

([1]) I kapitel IV anføres det, at »opt-in«-princippet på salgsstedet er en retlig forpligtelse, der allerede findes under databeskyttelsesdirektivet.