I

(Rezoluții, recomandări și avize)

AVIZE

AUTORITATEA EUROPEANĂ PENTRU PROTECȚIA DATELOR

Avizul Autorității Europene Pentru Protecția Datelor privind Comunicarea Comisiei către Parlamentul European, Consiliu, Comitetul Economic și Social European și Comitetul Regiunilor privind „Identificarea prin radiofrecvență (RFID) în Europa: etape în direcția elaborării unui cadru strategic", COM(2007) 96

(2008/C 101/01)

AUTORITATEA EUROPEANĂ PENTRU PROTECȚIA DATELOR,

având în vedere Tratatul de instituire a Comunității Europene, în special articolul 286,

având în vedere Carta Drepturilor Fundamentale a Uniunii Europene, în special articolul 8,

având în vedere Directiva 95/46/CE a Parlamentului European și a Consiliului din 24 octombrie 1995 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și libera circulație a acestor date,

având în vedere Directiva 2002/58/CE a Parlamentului European și a Consiliului din 12 iulie 2002 privind prelucrarea datelor personale și protejarea confidențialității în sectorul comunicațiilor publice,

având în vedere Regulamentul (CE) nr. 45/2001 al Parlamentului European și al Consiliului din 18 decembrie 2000 privind protecția persoanelor fizice cu privire la prelucrarea datelor cu caracter personal de către instituțiile și organele comunitare și privind libera circulație a acestor date și, în special, articolul 41,

ADOPTĂ PREZENTUL AVIZ:

I. **INTRODUCERE**

1. La 15 martie 2007, Comisia a adoptat o Comunicare privind „Identificarea prin radiofrecvență (RFID) în Europa: etape în direcția elaborării unui cadru strategic" [1] (denumită în continuare: „comunicarea"). În temeiul articolului 41 din Regulamentul (CE) nr. 45/2001, Autoritatea Europeană pentru Protecția Datelor (AEPD) este responsabilă de consilierea instituțiilor și a organismelor comunitare în toate chestiunile privind prelucrarea datelor cu caracter personal. În conformitate cu acest articol, AEPD își prezintă avizul.

2. Prezentul aviz trebuie văzut ca o reacție a AEPD la comunicare, precum și la alte acțiuni din domeniul RFID care s-au desfășurat după adoptarea comunicării. Celelalte acțiuni relevante care au fost luate în considerare în prezentul aviz includ:

   — decizia Comisiei din 28 iunie 2007 de instituire a grupului de experți în identificare prin radiofrecvență (RFID) [2], o consecință directă a comunicării. Acest grup este cunoscut ca Grupul părților interesate de RFID. În conformitate cu articolul 4 alineatul (4) litera (b) din decizie, AEPD participă la activitățile grupului în calitate de observator,

   — rezoluția Consiliului din 22 martie 2007 cu privire la o strategie pentru o societate informațională sigură în Europa [3],

   — proiectul „RFID și gestionarea identității", inițiat de Parlamentul European [4],

[1] COM(2007) 96 final.
[2] Decizia nr. 467/2007/CE (JO L 176, 6.7.2007, p. 25).
[3] JO C 68, 24.3.2007, p. 1.
[4] Proiectul „RFID și gestionarea identității — Studii de caz din avangarda dezvoltării către o inteligență ambiantă", comandat de Serviciul de evaluare științifică a opțiunii tehnologice (STOA) al Parlamentului European și realizat de către ETAG (Grupul european pentru evaluare tehnologică), http://www.europarl.europa.eu/stoa/default_en.htm

— adoptarea în iunie 2007 a Avizului nr. 4/2007 privind conceptul de date cu caracter personal de către Grupul de lucru „articolul 29" pentru protecția datelor ([1]),

— comunicarea Comisiei către Parlamentul European și Consiliu cu privire la continuarea programului de lucru pentru o mai bună punere în aplicare a directivei privind protecția datelor ([2]) și avizul AEPD privind această comunicare din 25 iulie 2007 ([3]),

— adoptarea de către Comisie a propunerii de directivă de modificare (inter alia) a Directivei 2002/58/CE privind prelucrarea datelor personale și protejarea confidențialității în sectorul comunicațiilor publice ([4]).

3. AEPD salută Comunicarea Comisiei privind RFID, deoarece aceasta abordează principalele probleme care apar în contextul instalării tehnologiei RFID, fără a neglija problemele esențiale cu privire la confidențialitate și protecția datelor. Această comunicare a beneficiat de un efort de pregătire constant și riguros. Într-adevăr, cinci ateliere tematice, precum și o consultare publică on-line ([5]) comandate de către Comisie au precedat această comunicare.

4. AEPD este de acord că sistemele RFID ar putea juca un rol cheie în dezvoltarea societății informaționale, de obicei numită „internetul obiectelor" și, de asemenea, împărtășește pe deplin îngrijorarea menționată la punctul 3.2 al comunicării, și anume că este posibil ca sistemele RFID să reprezinte o amenințare la adresa confidențialității datelor cu caracter personal și a drepturilor legate de protecția datelor. Într-adevăr, în raportul său anual pe 2005, AEPD a identificat RFID, alături de biometrie, mediile inteligenței ambiante și sistemele de gestionare a identității, ca evoluții tehnologice care sunt preconizate să aibă un impact major asupra protecției datelor.

5. Conform AEPD, adaptarea pentru uzul curent a tehnologiilor RFID și adoptarea lor pe scară largă nu numai că se vor realiza prin comoditatea lor atractivă sau prin serviciile pe care le oferă, dar vor fi, de asemenea, înlesnite prin beneficiile unor garanții solide și bine adaptate privind protecția datelor.

6. Pe scurt: AEPD califică RFID drept o evoluție tehnologică fundamental nouă, pe bună dreptate denumită, în comunicarea Comisiei, poarta spre o nouă etapă a dezvoltării societății informaționale.

7. Această evoluție ridică probleme importante în diferite domenii, unul dintre acestea fiind domeniul protecției datelor și al confidențialității. Avizul AEPD se limitează la acest domeniu.

II. ASPECTELE PRINCIPALE ALE AVIZULUI

8. Prezentul aviz se concentrează in special asupra posibilelor consecințe ale acestor evoluții cu privire la protecția datelor și confidențialitate. În acest moment aceste consecințe sunt nesigure, în parte datorită faptului că dezvoltarea sistemelor RFID și adaptarea lor pentru uzul curent sunt în plină evoluție și faptului că nu este clar unde se va încheia această dezvoltare.

9. Din această perspectivă, AEPD adoptă următoarea abordare:

— în primul rând, este necesară clarificarea consecințelor practice ale instalării sistemelor RFID în ceea ce privește protecția datelor și confidențialitatea,

— în al doilea rând, este necesară precizarea acestor consecințe, în contextul cadrului juridic existent privind protecția datelor și confidențialitatea,

— în al treilea rând, AEPD abordează întrebarea dacă aceste consecințe necesită reguli specifice pentru a aborda chestiunile privind protecția datelor pe care le implică utilizarea tehnologiilor RFID. Această problemă a fost deja ridicată de către AEPD în avizul său privind comunicarea cu privire la directiva privind protecția datelor și va fi elaborată mai în detaliu în prezentul aviz.

10. Prin adoptarea acestei abordări, AEPD intenționează să promoveze luarea în considerare a preocupărilor justificate cu privire la protecția datelor și confidențialitate în dezvoltarea sistemelor RFID și în adaptarea lor pentru uzul curent.

III. CLARIFICAREA CONSECINȚELOR

Sistemele și etichetele RFID

11. În ciuda faptului — deja menționat — că evoluțiile sunt în plină desfășurare și că rezultatul este nesigur, este foarte posibilă descrierea principalelor caracteristici ale acestor evoluții având în vedere consecințele lor cu privire la protecția datelor.

([1]) Document WP 136, publicat pe site-ul internet al grupului de lucru.
([2]) Comunicarea din 7 martie 2007 a Comisiei către Parlamentul European și Consiliu cu privire la continuarea programului de lucru pentru o mai bună punere în aplicare a directivei privind protecția datelor, COM(2007) 87 final.
([3]) JO C 255, 27.10.2007, p. 1. În continuare: „Avizul privind comunicarea cu privire la directiva privind protecția datelor".
([4]) Propunere din 13 noiembrie 2007 de directivă a Parlamentului European și a Consiliului de modificare a Directivei 2002/22/CE privind serviciile universale și drepturile utilizatorilor cu privire la rețelele și serviciile electronice de comunicații, a Directivei 2002/58/CE a Parlamentului European și a Consiliului din 12 iulie 2002 privind prelucrarea datelor personale și protejarea confidențialității în sectorul comunicațiilor publice și a Regulamentului (CE) nr. 2006/2004 privind cooperarea în materie de protecție a consumatorului, COM(2007) 698 final. Directiva 2002/58/CE este denumită în continuare „directiva privind confidențialitatea în mediul electronic".
([5]) http://www.rfidconsultation.eu/

12. În evaluarea potențialelor aspecte privind protecția datelor și confidențialitatea ale tehnologiei RFID, este extrem de relevant să fie luate în considerare nu numai etichetele RFID, ci și întreaga infrastructură RFID: eticheta, cititorul, rețeaua, baza de date de referință și baza de date în care sunt stocate datele produse de asocierea etichetă/cititor. După cum se subliniază pe scurt în introducerea comunicării, RFID nu înseamnă numai „etichete electronice", prin urmare chestiunile privind protecția datelor nu se vor limita exclusiv la etichete, ci vor cuprinde toate părțile infrastructurii de ansamblu a RFID. Într-adevăr, fiecare din aceste elemente are un rol în a contribui la punerea în aplicare a cadrului juridic european cu privire la protecția datelor, când este necesar. Acestea vor fi susținute de principalele tendințe din cadrul dezvoltării societății informaționale, cum ar fi lățimea de bandă aproape nelimitată, conexiuni de rețea ubicue și o capacitate de stocare nelimitată.

Impactul sistemelor și al etichetelor RFID

13. În ciuda nevoii unei abordări mai ample, după cum s-a subliniat în alineatul precedent, diferite motive justifică concentrarea în primul rând asupra utilizării RFID pentru etichetarea obiectelor în cazul produselor de larg consum, cum ar fi în sectorul de vânzare cu amănuntul. Motivul evident este că se prevede utilizarea sa sporită, care pare să se îndrepte spre aplicarea sa la scară largă. Contrar altor aplicații RFID cu utilizare redusă sau limitată, etichetarea la nivel de obiect are potențialul de a deveni o aplicație pentru utilizarea în masă. Multe produse de larg consum sunt deja prevăzute cu etichetă RFID. Legat de aceasta este faptul că o astfel de utilizare va afecta un număr enorm de persoane ale căror date cu caracter personal este probabil să fie prelucrate de fiecare dată când cumpără un produs care are o etichetă RFID.

14. Ar trebui acordată o atenție deosebită consecințelor etichetării RFID asupra deținătorilor de obiecte. Sistemele RFID ar putea extinde relația dintre un obiect și deținătorul acestuia. Odată ce această relație este extinsă, deținătorul poate fi scanat și clasificat ca fiind „cu venituri reduse" sau ca „țintă atractivă" pentru tranzacții viitoare; atribuirile unu-la-unu excesive ([1]) ar putea conduce la „pedepsirea" automată a unui anumit tip de comportament (obligația reciclării, deșeuri, etc.) Persoanele nu ar trebui să fie supuse la procesul de decizii automate potrivnice. Riscul ca societatea informațională să se îndrepte spre situația în care se vor lua decizii automate și în care se va abuza de tehnologie pentru a regulariza comportamentul uman devine tot mai mare, catalizat de această capacitate a RFID.

15. Datele stocate în sau furnizate de o etichetă RFID pot fi date cu caracter personal, astfel cum sunt definite la articolul 2 din directiva privind protecția datelor. De exemplu, cardurile inteligente de călătorie pot conține informații de identificare, precum și informații despre călătoriile recente ale deținătorului. Dacă o persoană fără scrupule ar dori să găsească pe cineva, ar fi suficient să plaseze în locurile potrivite cititori care ar oferi informații în legătură cu deplasările deținătorului cardului, astfel violând-le intimitatea și confidențialitatea informațiilor personale.

16. Amenințări similare la adresa confidențialității ar putea să apară chiar dacă informațiile stocate în eticheta RFID nu ar include numele persoanelor. Etichetele RFID conțin coduri unice de identificare atașate produselor de larg consum: dacă fiecare etichetă are un cod unic de identificare, o astfel de identificare poate fi utilizată în scop de supraveghere. De exemplu, dacă cineva poartă un ceas care are o etichetă RFID conținând un număr de identificare, acesta poate servi și ca identificator unic al deținătorului ceasului, chiar dacă identitatea acestuia nu este cunoscută. Directiva s-ar putea aplica sau nu, în funcție de modul în care sunt folosite informațiile — și în care sunt raportate fie la ceas, fie la persoană. Aceasta s-ar aplica, de exemplu, dacă se generează informații în legătură cu localizarea indivizilor, care ar putea să fie folosită pentru monitorizarea comportamentului acestora sau, de exemplu, pentru diferențierea prețurilor, interzicerea accesului sau expunerea nedorită la publicitate.

17. În acest context, este necesar să se asigure că aplicațiile RFID sunt instalate luând măsurile tehnologice necesare pentru minimizarea riscului de dezvăluire involuntară a informațiilor. Asemenea măsuri pot include necesitatea de a proiecta infrastructura RFID, în special etichetele RFID, într-un mod care să prevină un astfel de rezultat. De exemplu, etichetele RFID pot fi prevăzute cu o „comandă de oprire" („kill command") care să permită dezactivarea acestora. Această opțiune va fi discutată mai pe larg în capitolul IV al prezentului aviz.

18. Oferind posibilitatea de a urmări produsele după vânzare, sistemele RFID introduc noi probleme în dezbaterea privind confidențialitatea. Într-adevăr, în analiza impactului acestora, vor trebui luate în considerare două elemente: cât de personal este considerat obiectul și mobilitatea obiectului ([2]).

19. Ciclul de viață al unui obiect ar putea, de asemenea, complementa analiza solicitată a riscurilor și ar putea contribui la evaluarea cantitativă a amenințărilor potențiale la adresa confidențialității. Luând în considerare faptul este posibil ca o etichetă să nu poată fi dezactivată, un produs cu utilizator final care are un ciclu lung de viață va putea culege mai multe date conexe de la deținătorul produsului și construi un profil mai precis. Pe de altă parte, ciclul de viață scurt al unui obiect, cum ar fi o cutie de băuturi răcoritoare, de la fabricare până la etapa de reciclare ar putea prezenta mai puține riscuri și ar putea, așadar, necesita măsuri mai superficiale decât un produs cu un ciclu de viață mult mai lung.

([1]) Dr. Sarah Spiekermann, director al Centrului de cercetare privind economia internetului din Berlin, atelier pe tema RDIF și a calculării ubicue organizat de Dialogul transatlantic al consumatorilor, 13 martie 2007.

([2]) Dara J. Glasser, Kenneth W. Goodman and Norman G. Einspruch, „Chips, tags and scanners (Cipuri, etichete și scanere): Ethical challenges for radio frequency identification" (Provocările etice în identificarea prin radiofrecvență), Ethics and Information Technology, Volume 9, No 2/2007.

Chestiuni privind confidențialitatea și protecția datelor în instalarea sistemului RFID

20. Pentru a înțelege mai bine consecințele sistemelor RFID cu privire la confidențialitate și protecția datelor, se pot evidenția cinci probleme de bază în ceea ce privește confidențialitatea și protecția datelor.

21. Prima problemă este identificarea subiectului datelor. Cu mai bine de șaizeci de ani în urmă, scopul etichetei RFID era „identificarea prietenilor sau dușmanilor" care se apropie. Astăzi sistemele RFID pot nu numai să identifice elementele generale ale unui obiect, ci și, în cele din urmă, să conducă la identificarea unei persoane și, prin urmare, este necesar să facă acestea într-un mod care să permită protecției datelor.

22. A doua problemă este identificarea controlorului (controlorilor). În cazul sistemelor RFID, identificarea controlorului, astfel cum este definită la articolul 2 litera (d) din directiva privind protecția datelor, ar putea fi mai dificilă și, așadar, necesită o analiză mai amănunțită. Cu toate acestea, identificarea controlorului rămâne o etapă critică în stabilirea responsabilității fiecăruia din actorii relevanți care vor trebui să respecte cadrul juridic în materie de protecția datelor. În timpul ciclului de viață al unei etichete, controlorul care prelucrează datele s-ar putea schimba de mai multe ori în funcție de serviciile suplimentare care pot fi asigurate în legătură cu obiectul etichetat.

23. A treia problemă este reducerea diferenței tradiționale dintre sfera personală și cea publică. Deși diferența dintre spațiul privat și cel public nu a fost nici în trecut întotdeauna clar definită, majoritatea oamenilor sunt conștienți de hotarele dintre acestora (precum și de zonele gri) și iau decizii în cunoștință de cauză sau intuitive privind modul de acțiune adecvat. Potrivit lui Hall ([1]), spațiul personal este de obicei tradus prin distanța fizică față de ceilalți. Gestionarea confidențialității poate fi, de asemenea, considerată, un proces de reglementare a frontierelor dinamice ([2]). Prin urmare, nu este surprinzător faptul că tipul de conexiune fără fir („wireless") al comunicării prin etichete, precum și capacitatea sa de citire în afara razei vizuale, stârnesc preocupări privind confidențialitatea prin faptul că frontierele tradiționale și gestionarea acestora devin neclare. Într-adevăr, există temeri că persoana poate să-și piardă o parte sau tot controlul în ceea ce privește gestionarea distanței de care s-a bucurat până acum. Prin urmare, raza de citire a primelor sisteme RFID instalate a fost vizată în aceeași măsură de promotorii și de detractorii acestora.

24. A patra problemă trebuie să se ocupe de mărimea și proprietățile fizice ale etichetelor RFID. Deoarece este nevoie ca eticheta să fie mică și ieftină, măsurile de securitate care ar putea fi introduse în această porțiune a sistemului vor fi, prin definiție, limitate. Cu toate acestea, comunicarea fără fir adaugă, de asemenea, un set de riscuri prin comparație cu comunicarea prin fir și necesită, așadar, măsuri de securitate suplimentare.

25. A cincea problemă este lipsa de transparență a prelucrării datelor. Sistemele RFID pot conduce la colectarea și prelucrarea neobservate de informații care pot fi utilizate pentru crearea profilului unei persoane. Această consecință poate foarte ușor fi ilustrată prin compararea sistemelor RFID cu telefonul mobil, comparație care se face mai des. Pe de o parte, telefonul mobil a beneficiat de un nivel foarte ridicat de acceptare a tehnologiei, independent de potențialele riscuri de încălcare a confidențialității. S-ar putea trage concluzia că sistemele RFID vor fi acceptate în același mod. Pe de altă parte, trebuie subliniat faptul că un telefon mobil este un obiect vizibil care este, totuși, sub controlul utilizatorului final, de vreme ce poate fi închis. Lucrurile nu stau la fel în cazul RFID.

26. Deși colectarea și prelucrarea neobservate ale informațiilor menționate anterior pot fi legitime, este, de asemenea, posibil, iar în anumite situații chiar foarte probabil, să aibă loc colectarea și procesarea ilegitime ale unor astfel de date.

27. Clarificările acestui capitol justifică următoarea concluzie. Utilizarea pe scară largă a tehnologiei RFID este fundamental nouă și poate avea un impact fundamental asupra societății noastre și asupra protecției drepturilor fundamentale în societatea noastră, cum ar fi confidențialitatea și protecția datelor. Este posibil ca RFID să producă o schimbare calitativă.

IV. SPECIFICAREA CONSECINȚELOR

Introducere

28. Acest capitol se va concentra în special asupra impactului RFID asupra protecției drepturilor fundamentale în societatea noastră, cum ar fi confidențialitatea și protecția datelor. Acesta va fi precizat în două etape, prima fiind o scurtă descriere a modului în care aceste drepturi fundamentale sunt protejate în temeiul cadrului juridic actual. În a doua etapă, AEPD va discuta pe larg posibilitățile de a utiliza pe deplin cadrul juridic actual. Această dorință a fost introdusă în avizul privind comunicarea cu privire la directiva privind protecția datelor sub forma „punerii depline în aplicare a prezentelor dispoziții ale directivei".

29. Punctul de plecare este următorul: noile evoluții tehnologice, cum ar fi sistemele RFID, au un impact clar asupra cerințelor pentru un cadru juridic eficient în materie de protecția datelor. De asemenea, necesitarea protejării eficiente a datelor cu caracter personal ale persoanelor fizice poate impune limitări privind utilizarea acestor noi tehnologii. Astfel, interacțiunea este dublă: tehnologia influențează legislația, iar legislația influențează tehnologia ([3]).

([1]) Eduard T. Hall, The Hidden Dimension (Dimensiunea ascunsă) (prima ediție), Doubleday, Garden City, N.Y, 1966 Doubleday.

([2]) Altman, I., The Environment and Social Behaviour (Mediul și comportamentul social), Brooks-Cole, Monterrey, 1975.

([3]) A se vedea comentariile AEPD din martie 2006 cu privire la comunicarea Comisiei privind interoperabilitatea bazelor de date europene, publicate pe site-ul internet al AEPD.

Protecția drepturilor fundamentale

30. Protecția drepturilor fundamentale la confidențialitate și protecția datelor în cadrul Uniunii Europene este în primul rând garantată de un cadru juridic, care este necesar de vreme ce avem de a face cu drepturi care sunt recunoscute în temeiul articolului 8 al Convenției europene de apărare a drepturilor omului și a libertăților fundamentale, precum și în temeiul articolelor 7 și 8 ale Cartei Drepturilor Fundamentale a Uniunii. Cadrul juridic relevant pentru protecția datelor și RFID constă, de fapt, din Directiva 95/46/CE privind protecția datelor și din Directiva 2002/58/CE privind confidențialitatea în mediul electronic ([1]).

31. Cadrul juridic general pentru protecția datelor, astfel cum este prevăzut de Directiva 95/46/CE se aplică în cazul RFID, în măsura în care datele prelucrate de sistemele RFID intră sub incidența definiției datelor cu caracter personal. În timp ce, în anumite cazuri, aplicațiile RFID prelucrează în mod evident date cu caracter personal și se încadrează fără îndoială în sfera de aplicare a directivei privind protecția datelor, există aplicații pentru care aplicabilitatea directivei privind protecția datelor poate să nu mai fie atât de evidentă. Avizul nr. 4/2007 privind conceptul de date cu caracter personal al Grupului de lucru „articolul 29" pentru protecția datelor vizează să contribuie la o înțelegere mai clară și general acceptată a conceptului de date cu caracter personal și, prin aceasta, să diminueze această incertitudine ([2]).

32. În ceea ce privește directiva privind protecția confidențialității în mediul electronic, situația este următoarea. Până acum, nu este clar dacă această directivă se aplică aplicațiilor RFID. Din acest motiv, propunerea Comisiei din 13 noiembrie 2007 de modificare a directivei conține o dispoziție care vizează precizarea faptului că directiva se aplică, într-adevăr, anumitor aplicații RFID. Cu toate acestea, este posibil ca alte aplicații RFID să nu fie cuprinse datorită limitării acestei directive la prelucrarea datelor cu caracter personal legate de furnizarea de servicii de comunicații electronice accesibile publicului prin intermediul rețelelor de comunicații publice.

33. Protecția datelor cu caracter personal poate fi completată de o gamă de instrumente de autoreglementare (cadru nelegislativ). Utilizarea acestor instrumente este promovată activ în ambele directive, în special la articolul 27 din directiva privind protecția datelor care prevede că statele membre și Comisia încurajează elaborarea de coduri de conduită menite să contribuie la punerea în aplicare corectă a directivei. Mai mult, instrumentele de autoreglementare ar putea contribui în mod eficient la punerea în aplicare a măsurilor de securitate prevăzute la articolul 17 din directiva privind protecția datelor și la articolul 14 din directiva privind confidențialitatea în mediul electronic.

Aplicarea integrală a cadrului existent

34. Avizul privind comunicarea cu privire la Directiva privind protecția datelor enumeră o serie de instrumente disponibile pentru o mai bună punere în aplicare a directivei. Majoritatea instrumentelor fără caracter obligatoriu ale acestui aviz sunt relevante pentru RFID, cum ar fi comunicările interpretative sau alte comunicări, promovarea bunelor practici, utilizarea mărcilor de protecție a confidențialității și auditurile părților terțe privind confidențialitatea. Posibilitatea adoptării unor norme specifice pentru RFID va fi discutată în capitolul V. Dar sunt posibile îmbunătățiri și în cadrul existent.

Instrumente de autoreglementare

35. AEPD este de acord cu Comisia cu privire la faptul că într-o primă etapă este adecvat să se lase loc pentru autoreglementare, dând părților interesate posibilitatea de a crea un climat de respectare a legii și contribuind astfel la crearea unui cadru juridic mai sigur.

36. Se preconizează că, în consultare cu Grupul părților interesate de RFID, Comisia va stimula și coordona procesul de autoreglementare. În acest context, AEPD salută recomandarea anunțată în comunicare, care se preconizează că va conține orientări specifice care stabilesc „principiile pe care ar trebui să le aplice autoritățile publice și alte părți interesate cu privire la utilizarea RFID".

37. Comunicarea prevede că autoreglementarea va avea forma unui cod de conduită sau a unui cod de bune practici. Conform AEPD, indiferent de forma pe care o va avea autoreglementarea, aceasta ar trebui:

— să asigure orientare concretă și practică privind tipurile specifice de aplicații RFID și astfel să contribuie la respectarea cadrului juridic în materie de protecția datelor,

— să abordeze chestiunile și problemele specifice privind protecția datelor care se ivesc în contextul aplicațiilor RFID generale,

— să contribuie la aplicarea uniformă și armonioasă a directivei privind protecția datelor în UE, în special în sectoarele în care este probabil să se utilizeze același tip de aplicații RFID pe tot teritoriul UE,

— să fie aplicată de toate părțile interesate relevante. Nerespectarea acesteia ar trebui să aibă consecințe negative (posibil financiare).

([1]) Punctul 59 al prezentului aviz discută relevanța unei a treia directive, și anume Directiva 1999/5/CE a Parlamentului European și a Consiliului din 9 martie 1999 privind echipamentele hertziene și echipamentele terminale de telecomunicații și recunoașterea reciprocă a conformității acestora (JO L 91, 7.4.1999, p. 10).

([2]) A se vedea, *inter alia*, p. 10 din aviz, citată în nota de subsol 5.

38. AEPD subliniază o chestiune în cazul căreia autoreglementarea va fi utilă în mod deosebit. În cazul acelor aplicații RFID care implică prelucrarea de date cu caracter personal, directiva privind protecția datelor impune controlorilor de date diferite obligații, în special în temeiul articolului 17 (siguranța prelucrării) și în temeiul articolului 7 (necesitatea de a prelucra date numai având temeiuri juridice adecvate). În temeiul acestor dispoziții, controlorii de date trebuie, pe de o parte, să ia măsuri împotriva dezvăluirii neautorizate de date. Pe de altă parte, controlorii de date trebuie să asigure că prelucrarea, cum ar fi dezvăluirea de informații prin cititori, are loc, după caz, numai cu consimțământul în cunoștință de cauză al persoanei la care se referă datele.

39. Aceste dispoziții ale directivei privind protecția datelor pot fi interpretate că solicită ca aplicațiile RFID să fie instalate utilizând soluțiile tehnice necesare pentru a preveni sau minimiza riscurile de dezvăluire involuntară și pentru a asigura faptul că prelucrarea sau transferul de date are loc numai cu consimțământ în cunoștință de cauză, după caz. Din punctul de vedere al AEPD, existența unei astfel de obligații (și anume de a aplica soluțiile tehnice necesare pentru a preveni sau minimiza riscurile de dezvăluire involuntară) și caracterul său obligatoriu pentru instalatorii aplicațiilor RFID, va fi chiar mai puternică și mai clară dacă această cerință este preluată de viitorul cod de conduită sau cod de bune practici menționat anterior. Din aceste motive, AEPD recomandă cu tărie ca recomandarea Comisiei să includă o astfel de interpretare a directivei privind protecția datelor, subliniind existența unei obligații de a instala aplicații RFID luând măsurile tehnologice necesare pentru prevenirea colectării sau dezvăluirii involuntare de informații.

Necesitatea orientării

40. AEPD recomandă Comisiei ca, în cooperare strânsă cu grupul de experți RFID, să elaboreze unul sau mai multe documente care să ofere orientări clare privind modul de aplicare al cadrului juridic existent la mediul RFID. Orientarea ar trebui să prevadă modalități practice de respectare a principiilor stabilite de directiva privind protecția datelor și de directiva privind confidențialitatea în mediul electronic. În ceea ce privește abordarea generală a orientării și conținutul său concret, AEPD are următoarele sugestii:

41. Orientarea prin care se stabilesc principiile care se aplică cu privire la utilizarea RFID ar trebui să fie suficient de concentrată și să adopte o abordare specifică sectorului. O abordare de tipul „soluția universală” („one size fits all”) nu va realiza obiectivele dorite de asigurare a unui cadru clar și coerent. De aceea, domeniul de aplicare al orientării trebuie limitat la aplicații sectoriale RFID bine definite.

42. Mai mult, orientările ar trebui să propună metode practice eficiente pentru dezvoltarea *tehnicilor și standardelor* care ar putea contribui la respectarea de către sistemele RFID a cadrului juridic în materie de protecția datelor, fapt care va atrage după sine utilizarea unei tehnologii care implică „confidențialitate din concepție” („privacy by design”).

43. În aplicarea cadrului juridic existent mediului RFID, trebuie acordată o atenție deosebită punerii în aplicare a principiilor și obligațiilor privind protecția datelor care se aplică controlorilor de date din cadrul aplicațiilor RFID. Următoarele obligații și principii sunt deosebit de relevante:

— principiul dreptului la informații, inclusiv dreptul de a ști când se colectează date prin cititori și, în cazurile adecvate, când se etichetează produse,

— noțiunea de consimțământ ca temei juridic pentru prelucrarea datelor. Această noțiune se materializează în obligația de a dezactiva etichetele RFID la vânzare, cu excepția cazului în care subiectul datelor și-a dat consimțământul ([1]). Dreptul de a dezactiva etichetele RFID servește, de asemenea, scopului de a asigura securitatea informației, adică de a se asigura că datele prelucrate prin etichetele RFID nu sunt dezvăluite involuntar unor terțe părți,

— dreptul persoanelor fizice de a nu fi supuse unor decizii potrivnice bazate numai pe prelucrarea automată a unui profil personal definit.

44. În ceea ce privește dreptul la informații, orientarea ar trebui să stabilească faptul că persoanelor trebuie să li se furnizeze *informații* cu privire la prelucrarea datelor lor cu caracter personal. Acestea ar trebui, în special, atenționate, printre altele, cu privire: (i) la prezența cititorilor și a etichetelor RFID activate pe produse sau pe ambalajul acestora; (ii) la consecințele unei astfel de prezențe în termeni de colectare a informațiilor și (iii) la scopurile în care se intenționează să fie utilizate informațiile colectate.

45. Utilizarea unor sigle poate fi potrivită ca măsură de a oferi informații. Siglele pot fi utilizate pentru a atenționa asupra prezenței cititorilor și a etichetelor RFID care se presupune că rămân active. Cu toate acestea, numai utilizarea siglelor nu va fi suficientă pentru a asigura prelucrarea corectă a informațiilor care necesită ca informațiile să fie furnizate persoanelor vizate în mod clar și ușor de înțeles. Utilizarea siglelor ar trebui să fie considerată ca o măsură de completare a furnizării de informații mai detaliate.

([1]) A se vedea mai în detaliu punctele 46-50 ale prezentului aviz.

Piatra de temelie: Principiul consimțământului prealabil explicit („opt-in principle")

46. Pentru toate aplicațiile RFID relevante, soluțiile ar trebui să respecte și să pună în aplicare, ca o condiție necesară, principiul consimțământului prealabil explicit în momentul vânzării. Ar fi ilegal să se permită în continuare transmiterea de informații prin intermediul etichetelor RFID după momentul vânzării, cu excepția cazurilor în care controlorul de date are temei juridic adecvat. Temeiul juridic adecvat, în mod normal, ar fi: (a) consimțământul persoanei vizate sau (b) o solicitare specifică și liberă din partea persoanei vizate, dacă o asemenea dezvăluire este necesară pentru efectuarea unor servicii ([1]). Astfel ambele temeiuri juridice ar putea fi calificate ca respectând principiul consimțământului prealabil explicit.

47. În temeiul principiului consimțământului prealabil explicit, etichetele ar trebui dezactivate în momentul vânzării, cu excepția cazurilor în care persoana care a cumpărat obiectul la care este atașată eticheta dorește să o lase activată. Prin exercitarea dreptului de a o lăsa activată, persoana ar consimți la prelucrarea ulterioară a datelor sale, de exemplu, la transmiterea datelor către un cititor la vizita sa următoare la controlorul de date.

48. Pentru a face față creșterii diversității aplicațiilor RFID și pentru a facilita dezvoltarea unor modele inovatoare de afaceri, AEPD subliniază importanța unei abordări flexibile. Trebuie asigurată flexibilitate în ceea ce privește punerea în aplicare a principiului consimțământului prealabil explicit.

49. Opțiunile de punere în aplicare a principiului consimțământului prealabil explicit sunt multiple. De exemplu, ca alternativă la îndepărtarea etichetei, s-ar putea prevedea blocarea etichetei, scoaterea ei temporară din uz sau, folosind un model al politicii de securitate numit modelul „învierea rățuștei" („resurrecting duckling model") ([2]), blocată pentru folosirea numai de către un anumit utilizator. În cazul unei etichete cu un ciclu de viață scurt, adresa etichetei care trimite la informația stocată într-o bază de date ar putea fi, de asemenea, ștearsă din baza de date de referință, evitând continuarea prelucrării datelor suplimentare colectate prin etichetă.

50. Ca o concluzie, deși AEPD susține că principiul consimțământului prealabil explicit la momentul vânzării este o obligație legală deja existentă în majoritatea situațiilor în temeiul directivei privind protecția datelor, există motive întemeiate de a preciza această obligație în instrumente de auto-reglementare, pentru a asigura, de asemenea, faptul că principiul va fi pus în aplicare în modul cel mai adecvat. Punerea în aplicare specifică este, în orice caz, necesară în cazul acelor aplicații RFID care nu intră în domeniul de aplicare al directivei privind protecția datelor.

Necesitatea „confidențialității din concepție"

51. Pentru a minimiza amenințările la adresa confidențialității și a protecției datelor, comunicarea Comisiei susține, la punctul 3.2, pagina 6, ideea precizării și adoptării unor criterii timpurii de concepție. AEPD salută această abordare. Într-adevăr, adoptarea unor specificații și a unor criterii de concepție, cunoscute în general sub numele de „cele mai bune tehnici disponibile" (CBTD), va contribui în mod eficient la reglementarea protecției datelor și la cerințele de securitate. Identificarea criteriilor organizaționale și tehnologice, cu condiția revizuirii frecvente, va întări modelul de simbioză al cerințelor de confidențialitate și de securitate pe care îl dezvoltă Uniunea Europeană.

52. Definirea propriu-zisă a CBTD privind confidențialitatea și securitatea pentru sistemele RFID va fi, de asemenea, decisivă pentru construirea unui mediu de încredere, care va întări acceptarea la scară largă de către utilizatorii finali, precum și pentru competitivitatea industriei europene.

53. Procesul de selecționare a CBTD pentru sistemele RFID ar trebui să fie susținut de studii de impact asupra confidențialității și securității pentru care este încă necesar să se facă eforturi. AEPD consideră că Agenția europeană de securitate a rețelelor și a informațiilor (ENISA), împreună cu centrele comune de cercetare ale Comisiei Europene asociate cu părțile interesate relevante din industrie, poate contribui la identificarea celor mai bune practici și la elaborarea unor astfel de metodologii. Prin lansarea recentă a proiectului „orientări tehnice RFID", Biroul federal german pentru securitatea informațiilor (BSI) a dat un exemplu ilustrativ adecvat ([3]) de CBTD care ar trebui dezvoltate acum la nivel european.

54. Standardele pot, de asemenea, juca un rol decisiv în adoptarea timpurie a principiului „viață privată prin concepție". Așadar, Comisia ar trebui să contribuie la adoptarea unor garanții de confidențialitate și de protecția datelor în dezvoltarea unor standarde RFID internaționale. În documentul său ([4]) privind RFID, Grupului de lucru „articolul 29" a ilustrat clar posibilitatea ca standardele să contribuie la dezvoltarea sistemelor RFID într-un mod care să respecte confidențialitatea.

([1]) În cazul unor aplicații RFID, alte temeiuri pot fi posibile, cum ar fi articolul 7 litera (f) (interesul legitim al controlorului, sub rezerva unor garanții adecvate).

([2]) Numele acestui model elaborat de Frank Stajano și Ross Anderson de la Universitatea din Cambridge s-a inspirat din „felul în care un pui de gâscă care iese din ou presupune că primul obiect în mișcare pe care îl vede trebuie să fie mama sa".

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

([4]) Document de lucru (WP 105) privind chestiuni de protecția datelor conexe tehnologiei RFID, 19 ianuarie 2005.

55. Mai mult, AEPD salută poziția adoptată de Comisie cu privire la cercetarea și dezvoltarea tehnologiilor RFID și la necesitatea de a reduce riscurile la adresa confidențialității. Într-adevăr, principiul „confidențialitate din concepție" trebuie să fie introdus din cea mai timpurie etapă a dezvoltării tehnologiilor care vor contribui mai bine la respectarea cadrului juridic în materie de protecția datelor. Așa cum a prezentat pe scurt în raportul său anual pe 2006, AEPD se va alătura acestui efort prin avizele și consultanța pe care le asigură, de la caz la caz, proiectelor din cel de-al șaptelea Program-cadru (2007-2013).

V. SUNT NECESARE MĂSURI LEGISLATIVE SPECIFICE?

56. Este posibil ca autoreglementarea să nu fie suficientă ca mijloc de punere în aplicare deplină a cadrului existent în materie de protecția datelor și confidențialitate. Chiar dacă autoreglementarea îndeplinește cerințele menționate anterior, aplicarea sa este facultativă, iar nerespectarea acesteia nu poate fi întotdeauna sancționată eficient. În plus, este posibil să fie încă necesare măsuri legislative cu caracter obligatoriu, pentru a asigura protecția drepturilor persoanelor la confidențialitate și la protecția datelor. Acestea sunt cu atât mai necesare în cazul eșecului abordării prin autoreglementare.

57. O chestiune cheie este stabilirea instrumentelor juridice necesare pentru a se asigura faptul că aplicațiile RFID sunt instalate eficient utilizând soluțiile tehnice necesare pentru a preveni sau minimiza riscurile cu privire la protecția datelor și confidențialitate și că controlorii responsabili iau măsurile adecvate de respectare a obligațiilor care le revin în temeiul cadrelor juridice existente. Aceasta ridică câteva întrebări suplimentare:

— sunt necesare norme specifice?

— în cazul unei răspuns afirmativ, pot aceste norme fi adoptate în cadrul juridic existent, de exemplu utilizând procedurile de comitologie existente?

— sau este necesar un nou instrument legislativ pentru a asigura instalarea eficientă a aplicațiilor RFID utilizând tehnologii încorporate de protecție a confidențialității?

58. Acest capitol va aborda posibilitățile de a formula măsuri legislative cu caracter obligatoriu în cadrul juridic existent, în timp ce capitolul VI va discuta necesitatea unui nou instrument legislativ, deoarece aceasta este o chestiune diferită.

59. În primul rând, ar trebui acordată o atenție deosebită dispozițiilor articolului 17 din Directiva 95/46/CE, articolului 14 alineatul (3) din Directiva 2002/58/CE și articolului 3 alineatul (3) litera (c) din Directiva 1999/5/CE. Articolul 14 alineatul (3) permite statelor membre adoptarea de măsuri care să asigure faptul că echipamentele terminale sunt construite într-un mod care să le facă compatibile cu dreptul utilizatorilor de a proteja și de a controla folosirea datelor lor personale, în conformitate cu Directiva 1999/5/CE ([1]). La articolul 3 alineatul (3) litera (c), Directiva 1999/5/CE prevede că Comisia poate decide — prin procedura de comitologie — că aparatele din anumite clase de echipamente, sau aparatele de anumite tipuri sunt construite astfel încât să prezinte garanții pentru asigurarea protecției datelor cu caracter personal și a confidențialității utilizatorilor și a abonaților. Articolul 3 alineatul (3) litera (c) din Directiva 1999/5/CE nu a fost până acum utilizat.

60. Aceste dispoziții dau legiuitorului — la nivel național și comunitar — puterea de a prevedea faptul că garanțiile de confidențialitate și de protecția datelor trebuie să fie incluse în procesul de fabricație a sistemelor RFID, concept care este cunoscut drept „confidențialitate din concepție" ([2]). Aceasta necesită, de asemenea, utilizarea celor mai bune tehnici disponibile.

61. Pentru a face obligatoriu conceptul de „confidențialitate din concepție", AEPD recomandă Comisiei să utilizeze mecanismul de la articolul 3 alineatul (3) litera (c) din Directiva 1999/5/CE, în consultare cu grupul de experți RFID.

62. În al doilea rând, este posibilă specificarea aplicării cadrului juridic existent la RFID, prin modificări ale directivelor însele. După cum s-a spus deja, Comisia tocmai a prezentat o propunere de modificare a directivei privind confidențialitatea în mediul electronic care conține o dispoziție din această perspectivă. AEPD salută această primă confirmare a aplicabilității directivei la aplicațiile RFID. AEPD se va ocupa de aceste probleme specifice ridicate de relația dintre directiva privind confidențialitatea în mediul electronic și RFID în avizul său privind propunerea de modificare, care va fi dat la începutul anului 2008.

63. Luând în considerare faptul că Comisia nu prevede nicio modificare la directiva privind protecția datelor în viitorul apropiat ([3]), posibilitățile de specificare cu privire la aplicarea cadrului juridic existent la RFID sunt limitate.

VI. ESTE NECESAR UN CADRU JURIDIC SPECIFIC PRIVIND RFID?

Intențiile Comisiei

64. Comisia ([4]) subliniază importanța securității și a confidențialității din concepție. Aceasta necesită, de asemenea, implicarea tuturor părților interesate. Principalul rezultat al activităților Comisiei va fi „o recomandare prin care vor stabili

([1]) Și în conformitate cu Decizia nr. 87/95/CEE a Consiliului din 22 decembrie 1986 privind standardizarea în domeniul tehnologiei informației și telecomunicațiilor (JO L 36, 7.2.1987, p. 31).
([2]) A se vedea capitolul IV.
([3]) AEPD susține această abordare, a se vedea punctul 64.
([4]) A se vedea punctul 4.1 din comunicare.

principiile pe care autoritățile publice și alte părți interesate ar trebui să le aplice în materie de utilizare a RFID". Recomandarea va fi probabil adoptată în primăvara anului 2008. Ambițiile legislative menționate în comunicare conțin două etape. Comisia:

— va lua în considerare dispozițiile privind RFID în apropiata propunere de modificare a directivei privind confidențialitatea în mediul electronic. După cum s-a menționat anterior, în noiembrie 2007, Comisia a propus o astfel de modificare a directivei privind confidențialitatea în mediul electronic, care să confirme aplicabilitatea directivei la aplicațiile RFID ([1]), dar fără să propună lărgirea domeniului de aplicație a directivei privind confidențialitatea în mediul electronic la rețelele private,

— va evalua necesitatea unor etape legislative suplimentare pentru a garanta protecția datelor și confidențialitatea.

65. Aplicând această politică, se poate preconiza că Comisia nu are în plan — cel puțin pe termen scurt — propunerea unei noi legislații specifice pentru garantarea protecției datelor și a confidențialității în domeniul RFID.

Parametri pentru legiuitor

66. În avizul său cu privire la comunicarea privind directiva privind protecția datelor, AEPD a enumerat unele planuri de acțiuni legislative cu privire la prelucrarea datelor personale, care pot fi pot fi prezentate pe scurt după cum urmează:

— în primul rând, principiile de bază de protecția datelor ar trebui păstrate: „Nu sunt necesare noi principii, dar este clar că sunt necesare alte aranjamente administrative care, pe de o parte, sunt eficiente și adecvate unei societăți interconectate și care, pe de altă parte, minimizează costurile administrative" ([2]),

— în al doilea rând, propunerile legislative ar trebui înaintate numai dacă necesitatea și proporționalitatea sunt demonstrate suficient. Din acest motiv, pe termen scurt cadrul juridic general pentru protecția datelor nu ar trebui schimbat,

— în al treilea rând, evoluțiile în schimbare din societate pot duce la cadre juridice specifice, pentru a adapta principiile directivei privind protecția datelor la probleme ridicate de tehnologii specifice, cum ar fi RFID. Este clar că, în acest context, condițiile de necesitate și proporționalitate necesită, de asemenea, să fie îndeplinite.

67. Ca etapă următoare, este utilă specificarea așteptărilor cărora trebuie să le facă față legiuitorului în domeniul RFID:

— legislația trebuie să fie flexibilă și să lase loc inovațiilor și dezvoltării tehnologice. Aceasta ar trebui să conducă la legislație suficient de neutră din punct de vedere tehnologic,

— în al doilea rând, legislația trebuie să asigure certitudine juridică. Aceasta ar trebui să conducă la legislație suficient de specifică. Părțile interesate trebuie să știe precis cum le este reglementat comportamentul,

— în al treilea rând, legislația trebuie să protejeze în mod eficient toate interesele justificate aflate în joc. Aceasta necesită, în orice caz, aplicarea legislației și definirea clară a responsabilităților: care parte este responsabilă pentru un anumit comportament ([3])? Aceste cerințe sunt și mai importante în cazul în care sunt în joc confidențialitatea și protecția datelor, drepturile fundamentale ale persoanei în temeiul Convenției europene de apărare a drepturilor omului și a libertăților fundamentale și al Cartei Drepturilor Fundamentale a Uniunii.

Punctul de vedere al AEPD

68. Pentru AEPD, este clar că nu toate evoluțiile tehnologice ar trebui să conducă la reacții ale legiuitorului european. Dezvoltarea tehnologică poate fi rapidă, în timp ce adoptarea și intrarea în vigoare a legislației ia și ar trebui să ia timp. Legislația ar trebui să fie rezultatul echilibrării tuturor intereselor aflate în joc. Atunci când este aleasă directiva ca instrument, este necesar chiar mai mult timp, de vreme ce directivele trebuie puse în aplicare integral în sistemele juridice ale statelor membre.

69. Cu toate acestea, RFID nu este doar o altă evoluție tehnologică, cum s-a subliniat în câteva părți ale prezentului aviz. Comunicarea se referă la RFID ca la o poartă către o nouă fază de dezvoltare a societății informaționale, deseori menționată ca „internetul obiectelor", iar etichetele RFID vor constitui elemente-cheie ale mediilor „ambiante inteligente". Aceste medii constituie, de asemenea, etape în dezvoltarea a ceea ce este deseori denumită „societatea de supraveghere" ([4]). În acest context, acțiunea legislativă în domeniul RFID poate fi justificată. Este posibil ca RFID să producă o schimbare calitativă.

([1]) A se vedea noul articol 3 din Directiva 2002/58/CE.
([2]) Punctul 24 din Avizul cu privire la comunicarea privind directiva privind protecția datelor.
([3]) Introducerea terminologiei de protecție a datelor implică identificarea noțiunii de „controlor de date".
([4]) Acest mesaj a fost repetat într-o declarație a autorităților europene de protecție a datelor adoptată la Londra la 2 noiembrie 2006, disponibilă pe site-ul internet al AEPD: http://www.edps.europa.eu/EDPSWEB/edps/lang/en/pid/51

70. Din această perspectivă, AEPD recomandă luarea în considerare a adoptării (unei propuneri de) legislație comunitară care să reglementeze principalele probleme ale utilizării RFID în sectoarele relevante, în cazul în care punerea în aplicare propriu-zisă a cadrului juridic existent eșuează. După intrarea sa în vigoare, o astfel de măsură legislativă trebuie să fie considerată ca o „*lex specialis*" în ceea ce privește cadrul general în materie de protecția datelor.

71. Adoptarea unui astfel de instrument juridic ar avea următoarele avantaje:

— instrumentul ar stabili parametrii esențiali pentru mecanismele de autoreglementare,

— perspectiva adoptării unui instrument legislativ ar putea să se dovedească a fi un stimulent eficient pentru părțile interesate de stabilire a unor mecanisme de autoreglementare care să ofere o protecție precisă.

72. Pentru a face lucrurile mai practice, Comisiei i s-ar putea solicita să pregătească un document consultativ privind avantajele și dezavantajele unei legislații specifice și ale principalelor elemente ale unei astfel de legislații. Bineînțeles, părților interesate li s-ar putea solicita să-și aducă contribuția la această consultare. În mod similar, ar putea fi implicat Grupul de lucru „articolul 29".

Modalități posibile

73. Intervenția legiuitorului ar putea asigura un cadru legal adaptat, care să constea dintr-un amestec de instrumente de reglementare care specifică și completează cadrul juridic existent. Acest cadru legal adaptat ar trebui să se bazeze pe principiile cunoscute ale protecției datelor și ar trebui să se concentreze asupra diviziunii responsabilității și asupra eficienței mecanismelor de control.

74. Motivul specific pentru care o astfel de legislație adaptată ar putea fi necesară este legat de faptul că nu toate aplicațiile RFID aduc după sine prelucrarea de date personale. Cu alte cuvinte, dacă aplicațiile RFID nu aduc după sine prelucrarea de date personale, părțile implicate în fabricarea și vânzarea produselor bazate pe RFID nu sunt obligate din punct de vedere legal să pună în aplicare nicio măsură tehnologică care ar preveni interceptarea sau instalarea de cititori fără să anunțe ca atare persoanele. Totuși, după cum s-a demonstrat, riscurile la adresa confidențialității derivate din posibila supraveghere a persoanelor există, de asemenea, în cazul unor astfel de aplicații RFID, astfel necesitând același tip de garanții de confidențialitate. Aceasta poate fi valabil întocmai în cazul etichetării obiectelor la produsele de larg consum înainte de momentul vânzării. Pe scurt, aplicațiile RFID care nu prelucrează datele personale pot încă să amenințe confidențialitatea persoanelor prin posibilitatea de supraveghere ascunsă și prin utilizarea informațiilor în scopuri inacceptabile.

75. AEPD consideră că acest rezultat nefericit ar trebui evitat. Deoarece legislația actuală parțial nu reușește — cel puțin în cazul aplicațiilor RFID care nu prelucrează date personale — să contracareze această amenințare la adresa confidențialității și luând în considerare neajunsurile soluțiilor reprezentate de instrumentele juridice fără caracter obligatoriu, pare necesară recurgerea la unele măsuri legislative obligatorii pentru a asigura un rezultat satisfăcător.

76. În orice caz aceste măsuri ar trebui:

— să stabilească principiul consimțământului prealabil explicit la momentul vânzării ca obligație precisă care nu poate fi negată și în cazul aplicațiilor RFID care nu intră în domeniul de aplicare al directivei privind protecția datelor ([1]),

— să asigure instalarea obligatorie a aplicațiilor RFID având caracteristicile tehnice adecvate sau „confidențialitate din concepție".

VII. **CHESTIUNEA GUVERNANȚEI**

77. Deși dimensiunea „inerent transfrontalieră" a sistemelor RFID este văzută în comunicare ca ținând numai de piața internă, AEPD consideră că această dimensiune trebuie abordată la nivel internațional. Într-un magazin sistemele RFID sunt deja „transfrontaliere", de vreme ce activitatea unei etichete nu se oprește la momentul vânzării. La nivelul sistemului RFID global, aceste tehnologii devin, de asemenea, „transfrontaliere" atunci când ar putea avea loc transferul de date către o țară terță, în cazul în care producătorul obiectului etichetat care face parte din sistemul RFID are sediul în afara Uniunii Europene ([2]).

78. Din punct de vedere al perspectivei de viitor, guvernanța bazelor de date de referință a identității RFID reprezintă, de asemenea, o dimensiune critică pentru aplicarea adecvată a cadrului juridic european în materie de protecția datelor. AEPD îndeamnă să se găsească o soluție, deoarece degradarea în continuare a acestui cadru nu ar fi acceptabilă.

79. AEPD prevede faptul că problema guvernanței RFID va deveni o provocare majoră care va necesita investiții considerabile. Vor trebui găsite forumul de negociere potrivit, precum și infrastructura de gestionare cea mai adecvată, pentru a asigura respectarea adecvată a drepturilor de protecție a datelor în aceste medii internaționale.

([1]) Capitolul IV susține că principiul consimțământului prealabil explicit la momentul vânzării este o obligație legală deja existentă în temeiul directivei privind protecția datelor.

([2]) Obligațiile care revin din transferul de date personale sunt prevăzute la articolele 25 și 26 din directiva privind protecția datelor.

80. Din această perspectivă, AEPD invită Comisia să-și prezinte punctul de vedere cu privire la chestiunea guvernanței, posibil în consultare cu Grupul părților interesate de RFID.

VIII. **CONCLUZII**

81. AEPD salută Comunicarea Comisiei privind RFID deoarece aceasta abordează principalele probleme care apar în contextul instalării tehnologiei RFID, fără a neglija problemele principale cu privire la confidențialitate și protecția datelor. AEPD este de acord cu punctul de vedere care consideră că sistemele RFID ar putea juca un rol-cheie în dezvoltarea societății informaționale, cunoscută, de obicei, drept „internetul obiectelor".

Clarificarea consecințelor

82. Utilizarea pe scară largă a tehnologiei RFID este fundamental nouă și poate avea un impact fundamental asupra societății noastre și asupra protecției drepturilor fundamentale în societatea noastră, cum ar fi confidențialitatea și protecția datelor. Este posibil ca RFID să producă o schimbare calitativă.

83. Se pot deosebi cinci aspecte de bază privind problemele de confidențialitate și securitate:

— identificarea persoanei vizate,

— identificarea controlorului(controlorilor) de date,

— reducerea diferenței tradiționale dintre sfera personală și cea publică,

— consecințele mărimii și proprietăților fizice ale etichetelor RFID,

— lipsa de transparență a procesului.

Specificarea consecințelor

84. Cadrul juridic general pentru protecția datelor, astfel cum este prevăzut de Directiva 95/46/CE se aplică în cazul RFID, atât timp cât datele prelucrate de sistemele RFID intră sub incidența definiției datelor cu caracter personal.

85. În ceea ce privește directiva privind confidențialitatea în mediul electronic: Propunerea Comisiei din 13 noiembrie 2007 de modificare a directivei conține o dispoziție care vizează precizarea faptului că directiva se aplică, într-adevăr, anumitor aplicații RFID. Cu toate acestea, este posibil ca alte aplicații RFID să nu fie cuprinse datorită limitării acestei directive la prelucrarea datelor cu caracter personal legate de furnizarea de servicii de comunicații electronice accesibile publicului prin intermediul rețelelor de comunicații publice.

86. Protecția datelor cu caracter personal poate fi completată de o gamă de instrumente de autoreglementare (cadru nelegislativ). Este adecvat să se lase loc pentru autoreglementare, cu condiția ca:

— aceasta să asigure orientare concretă și practică privind tipurile specifice de aplicații RFID,

— aceasta să abordeze chestiunile și problemele specifice privind protecția datelor care se ivesc în contextul aplicațiilor RFID generale,

— aceasta să contribuie la aplicarea uniformă și armonioasă a directivei privind protecția datelor în UE,

— aceasta să fie aplicată de toate părțile interesate relevante.

87. AEPD recomandă Comisiei ca în cooperare strânsă cu grupul de experți RFID, să elaboreze unul sau mai multe documente care să ofere orientări clare privind modul de aplicare a cadrului juridic existent la mediul RFID.

88. Orientarea de stabilire a principiilor care se aplică cu privire la utilizarea RFID ar trebui să fie suficient de concentrată și să adopte o abordare specifică sectorului. Mai mult, orientările ar trebui să propună metode practice eficiente pentru dezvoltarea tehnicilor și standardelor care ar putea contribui la respectarea cadrului juridic în materie de protecția datelor de către sistemele RFID, fapt care va aduce după sine utilizarea tehnologiei „confidențialitate din concepție" („privacy by design").

89. AEPD salută abordarea din comunicarea Comisiei de a susține ideea precizării și adoptării timpurii a unor criterii de concepție.

90. Deși AEPD consideră că principiul consimțământului prealabil explicit la momentul vânzării este o obligație legală deja existentă în majoritatea situațiilor în temeiul directivei privind protecția datelor, această obligație ar trebui precizată în instrumente de autoreglementare.

Sunt necesare măsuri specifice?

91. Pentru a face obligatoriu conceptul de „confidențialitate din concepție", AEPD recomandă Comisiei să utilizeze mecanismul de la articolul 3 alineatul (3) litera (c) din Directiva 1999/5/CE, în consultare cu grupul de experți RFID.

92. Din această perspectivă, AEPD recomandă luarea în considerare a adoptării (unei propuneri de) legislație comunitară care să reglementeze principalele probleme ale utilizării RFID în sectoarele relevante, în cazul în care punerea în aplicare propriu-zisă a cadrului juridic existent ar eșua. După intrarea sa în vigoare, o astfel de măsură legislativă trebuie să fie considerată ca o „*lex specialis*" în ceea ce privește cadrul general în materie de protecția datelor. Această măsură legislativă ar trebui, de asemenea, să abordeze preocupările privind confidențialitate și protecția datelor care apar în cazul anumitor aplicații RFID, cum ar fi etichetarea obiectelor înainte de momentul vânzării, ceea ce este posibil să nu implice neapărat prelucrarea de date cu caracter personal.

93. Comisia ar trebui să pregătească un document consultativ privind avantajele și dezavantajele unei legislații specifice și ale principalelor elemente ale unei astfel de legislații.

94. Intervenția legiuitorului ar putea asigura un cadru legal adaptat, care să constea dintr-un amestec de instrumente de reglementare care specifică și completează cadrul juridic existent. În orice caz aceste măsuri ar trebui:

— să stabilească principiul consimțământului prealabil explicit la momentul vânzării ca obligație precisă care nu poate fi negată și în cazul aplicațiilor RFID care nu intră în domeniul de aplicare al directivei privind protecția datelor ([1]),

— să asigure instalarea obligatorie a aplicațiilor RFID având caracteristicile tehnice adecvate sau „confidențialitate din concepție".

Chestiunea guvernanței

95. AEPD invită Comisia să-și prezinte punctul de vedere cu privire la chestiunea guvernanței, pe cât posibil în consultare cu Grupul părților interesate de RFID.

Adoptat la Bruxelles, 20 decembrie 2007.

Peter HUSTINX

Autoritatea Europeană pentru Protecția Datelor

([1]) Capitolul IV susține că principiul consimțământului prealabil explicit la momentul vânzării este o obligație legală deja existentă în temeiul directivei privind protecția datelor.