I

(Rezoluții, recomandări și avize)

AVIZE

AUTORITATEA EUROPEANĂ PENTRU PROTECȚIA DATELOR

Avizul Autorității Europene pentru Protecția Datelor privind promovarea încrederii în societatea informațională prin încurajarea protecției datelor și a confidențialității

(2010/C 280/01)

AUTORITATEA EUROPEANĂ PENTRU PROTECȚIA DATELOR,

având în vedere Tratatul privind funcționarea Uniunii Europene, în special articolul 16,

având în vedere Carta drepturilor fundamentale a Uniunii Europene, în special articolele 7 și 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 ([1]),

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 electronice ([2]),

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 ([3]), în special articolul 41,

ADOPTĂ URMĂTORUL AVIZ:

I. **INTRODUCERE**

1. Tehnologiile informației și comunicațiilor (TIC) oferă posibilități extraordinare în aproape orice aspect al vieții noastre – modul în care muncim, ne distrăm, socializăm și învățăm. Acestea sunt esențiale pentru economia informațională de astăzi și pentru societate în general.

2. Uniunea Europeană este o forță globală în ceea ce privește progresul TIC și este hotărâtă să își păstreze poziția. Pentru a răspunde acestei provocări, Comisia Europeană este așteptată să adopte în curând o nouă Agendă digitală europeană pe care comisarul Kroes a confirmat-o ca fiind o prioritate de a sa ([4]).

3. AEPD recunoaște beneficiile datorate TIC și este de acord că UE ar trebui să facă tot posibilul pentru a impulsiona dezvoltarea și adoptarea lor la nivel general. Aceasta își manifestă pe deplin acordul față de opiniile comisarilor Kroes și Reding, potrivit cărora indivizii ar trebui să se afle în centrul acestui nou mediu ([5]). Aceștia ar trebui să aibă încredere în capacitatea TIC de a le păstra informațiile în siguranță și de a controla utilizarea lor, precum și să fie încredințați că drepturile lor la confidențialitate și la protecția datelor în spațiul digital vor fi respectate. Respectarea acestor drepturi este esențială pentru a câștiga încrederea consumatorilor. Iar această încredere este crucială dacă se dorește acceptarea acestor noi servicii de către cetățeni ([6]).

([1]) JO L 281, 23.11.1995, p. 31.
([2]) JO L 201, 31.7.2002, p. 37.
([3]) JO L 8, 12.1.2001, p. 1.

([4]) Răspunsuri la chestionarul Parlamentului European adresat comisarului Neelie Kroes în contextul audierilor PE care au precedat desemnarea comisarului.

([5]) Răspunsuri la chestionarul Parlamentului European adresat comisarului Neelie Kroes în contextul audierilor PE care au precedat desemnarea comisarului; discursul comisarului Viviane Reding cu privire la „O Agendă digitală europeană pentru noul consumator digital, oferit în cadrul Forumului pluripartit BEUC cu privire la confidențialitatea consumatorului și marketingul online: tendințele pieței și perspectivele politice", Bruxelles, 12 noiembrie 2009.

([6]) A se vedea, de exemplu, Raportul RISEPTIS, „Încrederea în societatea informațională", un raport al Comitetului consultativ, RISEPTIS (Cercetare și inovare privind securitatea, confidențialitatea și încrederea în societatea informațională). Disponibil la http://www.think-trust.eu/general/news-events/riseptis-report.html. A se vedea, de asemenea: J. B Horrigan, Adoptarea și utilizarea comunicațiilor în bandă largă în America, Inițiativa globală FCC privind comunicațiile în bandă largă, Documentul de lucru OBI, seria nr. 1.

4. UE dispune de un cadru juridic puternic cu privire la protecția datelor/confidențialitate, ale cărui principii rămân complet valabile în era digitală. Cu toate acestea, nu ne putem declara mulțumiți. În multe situații, TIC ridică noi preocupări care nu sunt incluse în cadrul existent. În consecință, trebuie adoptate măsuri pentru ca drepturile individuale, așa cum sunt consacrate în legislația UE, să asigure în continuare o protecție eficientă în acest nou mediu.

5. Prezentul aviz tratează măsurile care ar putea fi promovate sau adoptate de Uniunea Europeană pentru a garanta protecția datelor și a confidențialității persoanelor fizice într-o lume globalizată care va rămâne dependentă de tehnologie. Sunt dezbătute instrumentele legislative și nelegislative.

6. După o prezentare generală a TIC drept o nouă dezvoltare care creează oportunități, dar și riscuri, avizul dezbate necesitatea integrării, la nivel practic, a protecției datelor și a confidențialității chiar din faza conceperii noilor tehnologii ale informațiilor și comunicațiilor [principiul confidențialității prin concepție (*privacy by design*)]. Pentru a asigura respectarea acestui principiu, avizul dezbate necesitatea de a prevedea principiul confidențialității prin concepție în cadrul juridic privind protecția datelor în cel puțin două moduri diferite. În primul rând, prin includerea acestuia ca principiu general, obligatoriu, iar în al doilea rând, prin includerea acestuia în anumite domenii TIC, care prezintă riscuri specifice cu privire la protecția datelor/confidențialitate, ce pot fi diminuate printr-o arhitectură și printr-un design tehnic adecvat. Aceste domenii sunt identificarea prin radiofrecvență (RFID), aplicațiile pentru rețeaua de socializare și aplicațiile pentru browsere. În ultimul rând, avizul face sugestii cu privire la alte instrumente și principii menite să asigure confidențialitatea persoanelor fizice și protecția datelor din sectorul TIC.

7. În abordarea aspectelor sus-menționate, avizul dezvoltă câteva dintre observațiile Grupului de lucru al articolului 29 în ceea ce privește contribuția sa la consultarea publică despre viitorul confidențialității ([1]). Acesta se bazează în continuare pe avize anterioare ale AEPD, cum ar fi Avizul din 25 iulie 2007 privind punerea în aplicare a Directivei privind protecția datelor, Avizul din 20 decembrie 2007 privind RFID și cele două avize ale sale cu privire la Directiva privind confidențialitatea în mediul electronic ([2]).

II. TIC OFERĂ NOI OPORTUNITĂȚI, DAR PREZINTĂ ȘI NOI RISCURI

8. TIC au fost comparate cu alte invenții importante din trecut, cum ar fi energia electrică. Deși s-ar putea să fie prea devreme pentru a evalua impactul lor istoric real, legătura dintre TIC și dezvoltarea economică în țările dezvoltate este evidentă. TIC au dus la crearea de locuri de muncă, la beneficii economice și au contribuit la bunăstarea globală. Impactul TIC este mai mult decât economic, deoarece a jucat un rol important în stimularea inovării și a creativității.

9. Mai mult decât atât, TIC au transformat modul în care oamenii lucrează, socializează și interacționează. De exemplu, oamenii se bazează tot mai mult pe TIC în interacțiunile lor sociale și economice. Aceștia pot folosi o gamă largă de noi aplicații TIC precum e-sănătatea, e-transportul, e-guvernarea, precum și sisteme interactive inovatoare de divertisment și educație.

10. Având în vedere aceste beneficii, toate instituțiile europene și-au exprimat angajamentul de a sprijini TIC ca un instrument necesar pentru îmbunătățirea competitivității industriei europene și pentru accelerarea redresării economice a Europei. Într-adevăr, în august 2009, Comisia a adoptat Raportul privind competitivitatea digitală a Europei ([3]) și a lansat o consultare publică cu privire la strategiile viitoare de dezvoltare a TIC. La 7 decembrie 2009, Consiliul și-a prezentat contribuția la această consultare, denumită „Strategia Post i2010 – Către o societate deschisă, ecologică și competitivă, bazată pe cunoaștere” ([4]). Parlamentul

([1]) Avizul nr. 168 al Grupului de lucru al articolului 29 privind viitorul confidențialității, contribuție comună la Consultarea Comisiei Europene privind cadrul juridic al dreptului fundamental la protecția datelor cu caracter personal, adoptat la 1 decembrie 2009.

([2]) Avizul din 25 iulie 2007 privind 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, JO C 255, 27.10.2007, p. 1; Avizul din 20 decembrie 2007 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], JO C 101, 23.4.2008, p. 1; Avizul din 10 aprilie 2008 privind propunerea de directivă de modificare, printre altele, a Directivei 2002/58/CE privind prelucrarea datelor personale și protejarea confidențialității în sectorul comunicațiilor publice (Directiva privind confidențialitatea și comunicațiile electronice), JO C 181, 18.7.2008, p. 1; Al doilea aviz din 9 ianuarie 2009 cu privire la revizuirea Directivei 2002/58/CE privind prelucrarea datelor personale și protejarea confidențialității în sectorul comunicațiilor publice.

([3]) Raportul privind competitivitatea digitală a Europei – Principalele realizări ale strategiei i2010 în perioada 2005-2009, [SEC(2009) 1060].

([4]) Concluziile Consiliului „Strategia Post i2010 – Către o societate deschisă, ecologică și competitivă, bazată pe cunoaștere” (17107/09), adoptate la 18.12.2009.

European tocmai a adoptat un raport menit să orienteze Comisia în vederea stabilirii unei agende digitale ([1]).

11. Oportunitățile și beneficiile asociate dezvoltării TIC implică noi riscuri, în special în ceea ce privește confidențialitatea și protecția datelor cu caracter personal. TIC duce adesea la o proliferare (de multe ori în moduri imperceptibile de către indivizi) a cantității informațiilor colectate, sortate, filtrate, transferate sau altfel reținute și, în consecință, la amplificarea riscurilor legate de aceste date.

12. De exemplu, cipurile RFID înlocuiesc codurile de bare pentru (anumite) produse de larg consum. Îmbunătățind fluxul informațional din lanțul de aprovizionare (și reducând, astfel, necesitatea unor stocuri „de siguranță", asigurându-se previziuni mai exacte etc.), noul sistem este menit să avantajeze în aceeași măsură și întreprinderile și consumatorii. Astfel apare însă posibilitatea deranjantă de a fi urmărit, din diverse motive și de diferite entități, prin intermediul unor bunuri personale marcate.

13. Un alt exemplu îl reprezintă informatica dematerializată („cloud computing"), în esență, furnizarea de servicii de aplicații găzduite pentru consumatori și non-consumatori prin internet. Acestea variază de la galerii foto, agende electronice, webmail și baze de date pentru clienți până la servicii comerciale mai complexe. Avantajele pentru întreprinderi și persoane fizice sunt evidente; reducerea costurilor (costurile sunt în creștere), lipsa locației (acces ușor la informații oriunde în lume), automatizarea (nu este nevoie de resurse IT speciale și de actualizarea softwareului) etc. În același timp, riscurile unor probleme de securitate și ale pirateriei există și sunt foarte reale. Pierderea accesului la propriile date și a controlului asupra acestora este, de asemenea, un motiv de îngrijorare.

14. S-a dovedit că există avantaje și riscuri și în alte domenii care utilizează aplicații TIC. De exemplu, e-sănătatea, care poate spori eficacitatea, reduce costurile, mări accesibilitatea și duce la îmbunătățirea generală a calității serviciilor de sănătate. Cu toate acestea, e-sănătatea aduce adesea în discuție problema legitimității utilizărilor secundare ale informațiilor din acest domeniu, necesitând o analiză atentă a scopurilor oricărei posibile utilizări secundare ([2]). Mai mult decât atât, odată cu utilizarea tot mai largă a dosarelor medicale electronice, aceste sisteme au fost urmărite, la rândul lor, de scandaluri care au scos la iveală numeroase cazuri de piraterie asupra dosarelor medicale electronice.

15. Pe scurt, este posibil să persiste un anumit grad de risc, chiar și în urma realizării evaluărilor corecte și a aplicării măsurilor necesare. O situație în care riscurile sunt nule ar fi nerealistă. Totuși, așa cum se discută mai jos, aplicarea unor măsuri de reducere a acestor riscuri la un nivel corespunzător este posibilă și necesară.

III. **PRINCIPIUL CONFIDENȚIALITĂȚII PRIN CONCEPȚIE CA INSTRUMENT-CHEIE DE GENERARE A ÎNCREDERII ÎN TIC**

16. Beneficiile potențiale ale TIC pot fi valorificate în practică numai dacă pot genera încredere, cu alte cuvinte, dacă pot asigura dorința utilizatorilor de a se baza pe TIC datorită caracteristicilor și avantajelor lor. Această încredere este câștigată numai dacă TIC sunt fiabile, sigure, sub controlul indivizilor și dacă este garantată protecția datelor personale și confidențialitatea acestora.

17. Riscurile și neajunsurile larg răspândite precum cele ilustrate mai sus, în special atunci când duc la abuzul sau la încălcarea securității datelor cu caracter personal, expunând astfel viața privată a persoanelor, sunt susceptibile să submineze încrederea utilizatorilor în societatea informațională. Acest fapt ar putea pune serios în pericol dezvoltarea TIC și beneficiile pe care le-ar putea aduce.

18. Cu toate acestea, soluția la aceste riscuri pentru confidențialitate și protecția datelor nu poate fi eliminarea, excluderea sau refuzul de a utiliza sau de a promova TIC. Acest lucru nu ar fi nici posibil, nici realist; ar împiedica indivizii să se bucure de beneficiile TIC și ar limita serios avantajele globale care se pot obține.

19. AEPD consideră că o soluție mai pozitivă este conceperea și dezvoltarea TIC în așa fel încât confidențialitatea și protecția datelor să fie respectate. Astfel, este esențial ca protecția datelor și confidențialitatea să fie încorporate în întregul ciclu de viață al tehnologiei, de la prima fază de proiect până la desfășurarea, utilizarea și eliminarea lor. Acest proces este denumit, de obicei, confidențialitate prin concepție (CpC) și este prezentat pe larg în cele ce urmează.

20. CpC poate atrage după sine diferite acțiuni, în funcție de situația sau aplicația în cauză. De exemplu, în anumite cazuri, poate necesita eliminarea/reducerea datelor cu caracter personal sau evitarea prelucrărilor inutile și/sau nedorite. În alte cazuri, CpC poate duce la oferirea unor instrumente pentru sporirea controlului persoanelor fizice asupra datelor lor personale. Aceste măsuri ar trebui luate

([1]) Raport privind stabilirea unei noi Agende digitale pentru Europa: de la i2010 la digital.eu [2009/2225 (INI)], adoptat la18.3.2010.

([2]) De exemplu, vânzarea sau utilizarea de informații medicale colectate în scopul oferirii unui tratament nu poate fi utilizată pentru selectarea unor amplasamente pentru clinici-satelit, pentru înființarea unor centre ambulatorii de chirurgie sau pentru planificarea unor activități viitoare cu implicații financiare care ar necesita o examinare atentă.

în considerare la stabilirea standardelor și/sau a celor mai bune practici. Ele pot fi, de asemenea, incluse în arhitectura sistemelor de informare și de comunicare sau în organizarea structurală a entităților care prelucrează date cu caracter personal.

III.1. **Principiul confidențialității prin concepție aplicabil în diferite medii TIC și impactul acestora**

21. Se poate constata necesitatea aplicării principiului CpC în diferite medii TIC. De exemplu, sectorul sănătății se bazează tot mai mult pe infrastructurile TIC care determină adesea stocarea centralizată a informațiilor medicale ale pacienților. Aplicarea principiului CpC în sectorul sănătății ar necesita evaluarea caracterului adecvat al diferitelor măsuri, precum posibilitatea reducerii la minim a datelor stocate la nivel central sau a limitării acestora la un index, prin utilizarea unor instrumente de criptare, prin acordarea drepturilor de acces strict pe baza principiului cunoașterii strictului necesar, prin anonimizarea datelor odată ce acestea nu mai sunt necesare etc.

22. În mod similar, mijloacele de transport sunt tot mai mult prevăzute din construcție cu aplicații TIC avansate care interacționează cu vehiculul și cu mediul său în diferite scopuri și pentru diferite funcții. De exemplu, un număr tot mai mare de autovehicule sunt prevăzute cu noi dispozitive TIC (GPS, GSM, rețea de senzori etc.), care indică nu numai poziția acestora, ci și starea tehnică a autovehiculului în timp real. Aceste informații ar putea fi utilizate, de exemplu, pentru a înlocui actualul sistem de taxe rutiere cu o taxă de drum proporțională cu utilizarea acestuia. Aplicarea principiului CpC la proiectarea arhitecturii acestor sisteme ar susține prelucrarea și transferul unei cantități cât mai mici de date cu caracter personal ([1]). În conformitate cu acest principiu, este de preferat să se utilizeze, în locul arhitecturilor centralizate, arhitecturi descentralizate sau semi-descentralizate care limitează divulgarea datelor privind locația către un punct central.

23. Exemplele de mai sus arată că atunci când tehnologiile informațiilor și comunicațiilor sunt concepute în conformitate cu principiul CpC, riscurile pentru confidențialitate și protecția datelor pot fi diminuate semnificativ.

III.2. **Dezvoltarea insuficientă a TIC care aplică principiul CpC**

24. O problemă importantă o reprezintă măsura în care agenții economici, producătorii/furnizorii TIC și operatorii de date sunt sau nu interesați să comercializeze și să pună în aplicare principiul CpC în TIC. În acest context, este, de asemenea, important să se evalueze cererea utilizatorilor pentru CpC.

25. În 2007, Comisia a emis o comunicare prin care solicita întreprinderilor să își folosească puterea de inovare pentru a crea și a pune în aplicare PET ca mijloace de îmbunătățire a confidențialității și a protecției datelor personale chiar de la începutul ciclului de dezvoltare ([2]).

26. Cu toate acestea, până în prezent, datele disponibile indică faptul că nici producătorii de TIC, nici operatorii de date (din sectorul privat sau public) nu au reușit în mod constant să pună în aplicare sau să comercializeze CpC. Au fost invocate diferite motive, inclusiv lipsa unor stimulente economice sau a sprijinului instituțional, cererea insuficientă etc. ([3]).

27. În același timp, cererea utilizatorilor pentru CpC a fost destul de scăzută. Utilizatorii de produse și servicii TIC sunt îndreptățiți să presupună că viața privată și datele lor personale sunt protejate *de facto*, când, foarte adesea, acest lucru nu se întâmplă. În unele cazuri, aceștia nu sunt, pur și simplu, în măsură să adopte măsurile de securitate necesare pentru protecția datelor lor personale sau ale altora. De multe ori, acest lucru se întâmplă deoarece nu cunosc în întregime și nici măcar parțial riscurile. De exemplu, în general, tinerii nu țin seama de riscurile pentru viața privată pe care le implică afișarea unor informații personale pe rețelele de socializare și ignoră setările de siguranță. Alți utilizatori sunt conștienți de riscuri, dar este posibil să nu aibă expertiza tehnică necesară pentru a pune în aplicare tehnologiile de siguranță, precum cele care asigură protecția conexiunii lor la internet sau modalitatea de modificare a setărilor browserului pentru a reduce la minim posibilitatea realizării unui profil prin monitorizarea activităților lor de navigare pe internet.

28. Cu toate acestea, riscurile pentru confidențialitate și protecția datelor sunt foarte reale. În cazul în care nu se are de la bun început în vedere confidențialitatea și protecția datelor cu caracter personal, de multe ori este prea târziu și prea dificil din punct de vedere economic ca sistemele să fie consolidate și prea târziu ca daunele deja

([1]) A se vedea Avizul Autorității Europene pentru Protecția Datelor din 22 iulie 2009 privind Comunicarea Comisiei cu privire la un Plan de acțiune pentru implementarea sistemelor de transport inteligente în Europa și propunerea însoțitoare de Directivă a Parlamentului European și a Consiliului de instituire a cadrului pentru implementarea sistemelor de transport inteligente în domeniul transportului rutier și pentru interfețele cu alte moduri de transport, disponibil la: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2009/09-07-22_Intelligent_Transport_Systems_RO.pdf

([2]) Comunicarea Comisiei COM(2007) 228 final către Parlamentul European și Consiliu din 2.5.2007 privind promovarea protecției datelor prin intermediul tehnologiilor pentru consolidarea confidențialității (*privacy enhancing technologies* – PET).

([3]) Studiu privind beneficiile economice ale tehnologiilor pentru consolidarea confidențialității (PET) jls/2008/D4/036.

create să fie reparate. Frecvența tot mai mare a cazurilor de încălcare a securității datelor din ultimii ani ilustrează perfect această problemă și subliniază și mai mult necesitatea de a proteja confidențialitatea încă din faza de proiect.

29. Argumentele de mai sus sugerează în mod clar că producătorii și furnizorii de tehnologii TIC menite să prelucreze datele cu caracter personal ar trebui să aibă, împreună cu operatorii de date, responsabilitatea de a prevedea dispozitive de securitate integrate care să asigure protecția datelor și confidențialitatea. În multe cazuri, aceasta înseamnă că ele ar trebui prevăzute cu setări de confidențialitate prestabilite.

30. În acest context, trebuie să avem în vedere măsurile care trebuie luate de responsabilii politici în vederea promovării principiului CpC în dezvoltarea TIC. O primă întrebare este legată de măsura în care cadrul juridic existent cu privire la protecția datelor conține prevederi adecvate pentru asigurarea punerii în aplicare a principiului CpC atât de către operatorii de date, cât și de producători/dezvoltatori. O a doua întrebare se referă la acțiunile care ar trebui întreprinse în contextul Agendei digitale europene pentru a asigura generarea încrederii consumatorilor în sectorul TIC.

IV. **INCLUDEREA PRINCIPIULUI CONFIDENȚIALITĂȚII PRIN CONCEPȚIE ÎN LEGISLAȚIA ȘI POLITICILE UE**

IV.1. **Cadrul juridic actual privind protecția datelor și confidențialitatea**

31. UE are un cadru juridic solid cu privire la protecția datelor și confidențialitate, consacrat în Directiva 95/46/CE ([1]), în Directiva 2002/58/CE ([2]) și în jurisprudența Curții Europene a Drepturilor Omului ([3]) și a Curții de Justiție.

32. Directiva privind protecția datelor se aplică „oricărei operațiuni sau serii de operațiuni care se efectuează asupra datelor cu caracter personal” (colectarea, stocarea, dezvăluirea etc.). Aceasta impune respectarea anumitor principii și obligații de către operatorii care prelucrează date personale („operatorii de date”). Ea stabilește drepturile individuale, precum dreptul de a accesa informații personale. Directiva privind confidențialitatea în mediul electronic tratează în mod specific chestiunea protecției confidențialității în sectorul comunicațiilor electronice ([4]).

33. Actuala directivă privind protecția datelor nu cuprinde o cerință explicită în ceea ce privește CpC. Cu toate acestea, include prevederi care pot necesita indirect, în diferite situații, punerea în aplicare a principiului CpC. Articolul 17 în special le impune operatorilor de date să pună în aplicare măsuri tehnice și organizatorice adecvate pentru a preveni prelucrarea ilegală a datelor ([5]). Astfel, principiul CpC este tratat într-un mod foarte generic. Mai mult, prevederile directivei se adresează în principal operatorilor de date și se referă la prelucrarea de către aceștia a informațiilor personale. Acestea nu solicită în mod explicit ca tehnologiile informațiilor și comunicațiilor să respecte condițiile legate de confidențialitate și de protecția datelor, care necesită, de asemenea, implicarea proiectanților și producătorilor de TIC, inclusiv activitățile realizate în faza de standardizare.

34. Directiva privind confidențialitatea în mediul electronic este mai explicită. Articolul 14 alineatul (3) prevede că „Dacă este necesar, se pot adopta măsuri care să asigure 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 și cu Decizia 87/95/CEE a Consiliului din 22 decembrie 1986 privind standardizarea în domeniul tehnologiei informațiilor și al comunicațiilor”. Totuși, această prevedere nu a fost niciodată utilizată ([6]).

35. Deși prevederile de mai sus ale celor două directive contribuie la *promovarea* principiului confidențialității prin concepție, practic, ele nu au fost suficiente pentru *a asigura* includerea confidențialității în TIC.

36. Ca urmare a situației de mai sus, legislația nu impune suficient de explicit ca TIC să fie concepute în conformitate cu principiul CpC. De asemenea, autoritățile pentru protecția datelor nu au suficiente competențe pentru a asigura includerea principiului CpC. Aceasta duce la ineficiență. De exemplu, autoritățile pentru protecția datelor pot impune sancțiuni în cazul în care nu se răspunde la cererile de acces din partea persoanelor fizice și vor putea solicita punerea în aplicare a anumitor măsuri pentru a preveni prelucrarea ilegală a datelor. Cu

([1]) Directiva 95/46/CE a Parlamentului European și a Consiliului (în continuare: Directiva privind protecția datelor).

([2]) Directiva 2002/58/CE a Parlamentului European și a Consiliului (în continuare: Directiva privind confidențialitatea în mediul electronic).

([3]) Interpretarea principalelor elemente și condiții prevăzute la articolul 8 al Convenției Europene privind protecția drepturilor omului și a libertăților fundamentale (CEDO) adoptată la Roma la 4 noiembrie 1950, așa cum se aplică în cazuri diferite.

([4]) Tratatul de la Lisabona a întărit această protecție prin recunoașterea respectării confidențialității și protecția datelor cu caracter personal ca drepturi fundamentale distincte în articolele 7 și 8 din Carta drepturilor fundamentale a UE. Carta drepturilor fundamentale a UE a devenit obligatorie odată cu intrarea în vigoare a Tratatului de la Lisabona.

([5]) Articolul 17 este formulat după cum urmează: „Statele membre prevăd aplicarea obligatorie de către operator a unor măsuri tehnice și organizatorice de protecție adecvate pentru protejarea datelor cu caracter personal împotriva distrugerii accidentale sau ilegale, pierderii accidentale, modificării, dezvăluirii sau accesului neautorizat, în special atunci când prelucrarea presupune transmiterea datelor într-o rețea, precum și împotriva oricărei alte forme de prelucrare ilegală.” Considerentul 46 îl completează după cum urmează: „întrucât protecția drepturilor și libertăților persoanelor vizate în ceea ce privește prelucrarea datelor cu caracter personal necesită luarea unor măsuri tehnice și organizatorice adecvate atât în momentul proiectării sistemului de prelucrare, cât și în cel al prelucrării în sine, în special în scopul menținerii securității și prevenirii oricărei prelucrări neautorizate”.

([6]) Comisia și-a anunțat intenția de a actualiza Directiva 1999/5/CE spre sfârșitul anului 2010.

toate acestea, nu este întotdeauna suficient de clar dacă autoritatea acestora se extinde la impunerea conceperii unui sistem care să faciliteze drepturile persoanelor fizice de protecție a datelor ([1]). De exemplu, pe baza prevederilor legale existente, nu este clar dacă se poate solicita conceperea unei arhitecturi a sistemului informațional în așa fel încât aceasta să faciliteze răspunsul companiilor la cererile de accesare a datelor din partea persoanelor fizice astfel încât acestea să fie tratate automat și mai rapid. În plus, încercările ulterioare de modificare a tehnologiei odată ce aceasta a fost dezvoltată sau perfecționată pot duce la un amalgam de soluții care, pe lângă faptul că sunt oneroase, nu sunt complet funcționale.

37. În opinia AEPD, care este împărtășită de Grupul de lucru al articolului 29 ([2]), cadrul juridic actual lasă loc pentru o susținere mai explicită a principiului CpC.

IV.2. **Includerea principiului confidențialității prin concepție la diferite niveluri**

38. Având în vedere cele de mai sus, AEPD recomandă Comisiei să urmeze 4 planuri de acțiune:

(a) să propună includerea unei prevederi generale cu privire la principiul CpC în cadrul juridic privind protecția datelor;

(b) să dezvolte această prevedere generală în prevederi specifice, atunci când sunt propuse instrumente juridice specifice în diferite sectoare. Este posibil ca aceste prevederi specifice să fie deja incluse în instrumente juridice, pe baza articolului 17 din Directiva privind protecția datelor (și a altor legi existente);

(c) să includă principiul CpC ca principiu director în Agenda digitală europeană;

(d) să introducă principiul CpC în alte inițiative UE (în special inițiative nelegislative).

O prevedere generală privind CpC

39. AEPD propune includerea univocă și explicită a principiului confidențialității prin concepție în cadrul de reglementare existent privind protecția datelor. Astfel, principiul CpC ar fi mai puternic, mai explicit și va obliga la aplicarea sa efectivă, pe lângă faptul că va oferi o mai mare legitimitate autorităților de aplicare a legii să impună aplicarea sa *de facto*. Acest fapt este în special necesar având în vedere cele prezentate mai sus, nu numai importanța principiului în sine ca instrument de promovare a încrederii, ci și ca stimulent pentru părțile interesate de a pune în aplicare CpC și de a mări garanțiile prevăzute în cadrul juridic existent.

40. Această propunere are la bază recomandarea Grupului de lucru al articolului 29 de introducere a principiului confidențialității prin concepție ca principiu general în cadrul juridic privind protecția datelor în special în Directiva privind protecția datelor. În conformitate cu Grupul de lucru al articolului 29: „Acest principiu ar trebui să fie obligatoriu pentru proiectanții și producătorii de tehnologii, precum și pentru operatorii de date care trebuie să ia hotărâri cu privire la achiziționarea și utilizarea TIC. Aceștia ar trebui să fie obligați să țină seama de protecția datelor tehnologice încă din faza de proiectare a procedurilor și sistemelor tehnologice de informare. Furnizorii de astfel de sisteme sau servicii și operatorii de date ar trebui să demonstreze că au luat toate măsurile necesare pentru respectarea acestor cerințe.”

41. AEPD salută, de asemenea, acordul comisarului Viviane Reding în ceea ce privește principiul confidențialității prin concepție, în contextul anunțării revizuirii Directivei privind protecția datelor ([3]).

42. Ajungem astfel la conținutul acestui regulament. În primul rând, principiul general al confidențialității prin concepție ar trebui să fie neutru din punct de vedere tehnologic. Principiul nu ar trebui să urmărească reglementarea tehnologiei, adică nu ar trebui să prescrie soluții tehnice specifice, ci să prevadă integrarea principiilor existente privind confidențialitatea și protecția datelor în sistemele și soluțiile de informare și comunicare. Astfel, părțile interesate, producătorii, operatorii de date și autoritățile pentru protecția datelor ar putea interpreta înțelesul principiului în fiecare caz în parte. În al doilea rând,

([1]) A se vedea Raportul Biroului Comisarului pentru Informații din Regatul Unit denumit „Privacy by Design” (*Confidențialitatea prin concepție*), publicat în noiembrie 2008.

([2]) A se vedea Avizul nr. 168 al Grupului de lucru al articolului 29 privind viitorul confidențialității, contribuție comună la Consultarea Comisiei Europene cu privire la cadrul juridic al dreptului fundamental la protecția datelor cu caracter personal, adoptat la 1 decembrie 2009.

([3]) Confidențialitatea prin concepție este un principiu atât în interesul cetățenilor, cât și al întreprinderilor. Acesta va duce la o protecție sporită a persoanelor și la creșterea încrederii în noile servicii și produse, ceea ce va avea, la rândul său, un impact pozitiv asupra economiei. Există o serie de exemple încurajatoare, însă mai sunt multe de făcut. Discurs de deschidere cu ocazia Zilei pentru protecția datelor – 28 ianuarie 2010, Parlamentul European, Bruxelles.

respectarea principiului ar trebui să fie obligatorie în diferite faze, de la crearea standardelor și conceperea arhitecturii până la punerea lor în aplicare de către operatorul de date.

Prevederi în instrumente juridice specifice

43. Instrumentele legislative actuale și viitoare trebuie să includă principiul CpC pe baza cadrului juridic existent, iar după adoptarea prevederilor generale propuse mai sus, pe baza acestora din urmă. De exemplu, conform actualelor inițiative privind sistemele de transport inteligent, Comisia va avea o responsabilitate inițială specifică în ceea ce privește stabilirea măsurilor, a inițiativelor de standardizare, a procedurilor și a celor mai bune practici. În executarea acestor sarcini, CpC ar trebui să fie un principiu director.

44. AEPD remarcă, de asemenea, că principiul confidențialității prin concepție are o importanță deosebită în domeniul libertății, securității și justiției, în special în ceea ce privește obiectivele strategiei de gestionare a informațiilor, așa cum sunt prevăzute în Programul de la Stockholm ([1]). În avizul său cu privire la Programul de la Stockholm, AEPD a subliniat că arhitectura schimbului de informații ar trebui să aibă la bază principiul confidențialității prin concepție ([2]): „Aceasta înseamnă, mai concret, că sistemele informaționale menite să asigure securitatea publică ar trebui să fie întotdeauna construite în conformitate cu principiul confidențialității prin concepție."

45. Avizul Grupului de lucru al articolului 29 cu privire la viitorul confidențialității ([3]) insistă în termeni și mai preciși că în domeniul libertății, securității și justiției – în care autoritățile publice sunt principalii actori și în care măsurile de sporire a controlului au un impact direct asupra drepturilor fundamentale privind confidențialitatea și protecția datelor – cerințele legate de confidențialitatea prin concepție ar trebui să fie obligatorii. Prin introducerea acestor cerințe în sistemele informaționale, guvernele ar stimula la rândul lor utilizarea principiului confidențialității prin concepție în calitatea lor de primi clienți.

CpC ca principiu director în cadrul Agendei digitale europene

46. Tehnologiile informațiilor și comunicațiilor sunt tot mai complexe și determină riscuri mai mari în ceea ce privește protecția datelor și confidențialitatea. În general, informațiile digitalizate, care sunt mai ușor de accesat, de copiat și de transmis, sunt expuse unor riscuri mai mari decât informațiile pe suport de hârtie. Pe măsură ce ne îndreptăm spre rețelele de obiecte interconectate, riscurile vor fi tot mai mari. Cu cât sunt mai mari riscurile pentru viața privată/protecția datelor, cu atât cresc și cerințele pentru creșterea securității protecției datelor/confidențialității. În consecință, justificarea necesității punerii în aplicare a principiului CpC este mai riguroasă în sectorul TIC. În plus, așa cum s-a discutat mai sus, încrederea persoanelor în TIC este fundamentală dacă se dorește adoptarea acestor noi servicii de către cetățeni, iar confidențialitatea și protecția datelor sunt elemente esențiale pentru câștigarea acestei încrederi.

47. Cele de mai sus subliniază faptul că o strategie pentru dezvoltarea TIC trebuie să confirme necesitatea conceperii acestora cu un element inerent de confidențialitate și protecție a datelor, adică să se țină seama de principiul confidențialității prin concepție.

48. În consecință, Agenda digitală europeană ar trebui să susțină în mod explicit principiul confidențialității prin concepție ca element necesar pentru asigurarea încrederii cetățenilor în TIC și în serviciile on-line. Ar trebui să recunoască faptul că încrederea și confidențialitatea merg mână în mână și că principiul confidențialității prin concepție ar trebui să fie un factor director în dezvoltarea unui sector TIC de încredere.

CpC ca principiu în cadrul altor inițiative ale UE

49. Comisia ar trebui să considere confidențialitatea prin concepție un principiu director în punerea în aplicare a politicilor, activităților și inițiativelor sale în sectoare specifice ale TIC, inclusiv e-sănătatea, achizițiile publice electronice, asigurările sociale electronice, eLearning etc. Multe dintre aceste inițiative vor constitui acțiuni în cadrul Agendei digitale europene.

50. Aceasta înseamnă, de exemplu, că inițiativele menite să asigure creșterea eficacității și a modernității aplicațiilor guvernamentale astfel încât persoanele să poată interacționa cu administrațiile ar trebui să includă necesitatea ca acestea să fie elaborate și utilizate în conformitate cu principiul confidențialității prin concepție. Același lucru este valabil și pentru politicile și activitățile Comisiei care urmăresc furnizarea unor servicii de internet mai rapide, a unui conținut digital mai rapid sau încurajarea la nivel general a comunicațiilor fixe și mobile și a transmisiilor de date.

([1]) Programul de la Stockholm – O Europă deschisă și sigură în serviciul cetățenilor și pentru protecția acestora, aprobat de Consiliul European în decembrie 2009.

([2]) Avizul din 10 iulie 2009 privind Comunicarea Comisiei către Parlamentul European și Consiliu privind un spațiu de libertate, securitate și justiție în serviciul cetățenilor, JO C 276, 17.11.2009, p. 8, pct. 60.

([3]) Avizul Grupului de lucru al articolului 29 privind viitorul confidențialității, contribuție comună la Consultarea Comisiei Europene cu privire la cadrul juridic al dreptului fundamental la protecția datelor cu caracter personal, adoptat la 1 decembrie 2009.

51. Cele de mai sus includ, de asemenea, domeniile în care Comisia este responsabilă pentru sistemele informatice la scară largă, cum ar fi SIS și VIS, precum și cazurile în care responsabilitatea Comisiei se limitează la dezvoltarea și la menținerea infrastructurii comune a unui astfel de sistem, cum ar fi Sistemul european de informații cu privire la cazierele judiciare (ECRIS).

52. Modul în care principiul CpC va fi dezvoltat depinde de fiecare sector și situație în parte. De exemplu, atunci când inițiativele Comisiei sunt însoțite de propuneri legislative cu privire la un anumit sector TIC, se va dovedi de multe ori necesară includerea unei trimiteri explicite la noțiunea CpC aplicabilă sistemului/aplicației TIC în cauză. În cazul în care sunt concepute planuri de acțiune pentru un anumit domeniu, acestea ar trebui să asigure în mod sistematic aplicarea cadrului juridic și, mai precis, să garanteze faptul că tehnologia TIC a fost concepută ținându-se seama de principiul confidențialității prin concepție.

53. În ceea ce privește cercetarea, Al șaptelea program-cadru și cele ulterioare ar trebui utilizate ca instrumente de susținere a proiectelor care urmăresc analizarea standardelor, a tehnologiilor și arhitecturii TIC care asigură mai bine confidențialitatea și, în special, principiul confidențialității prin concepție. În plus, CpC ar trebui să fie și un element necesar de care să se țină seama în proiectele TIC mai ample care vizează prelucrarea datelor cu caracter personal ale persoanelor fizice.

Domenii de interes specific

54. În unele cazuri, din cauza riscurilor specifice pentru confidențialitate și protecția datelor persoanelor fizice sau din cauza altor factori (refuzul industriei de a furniza produse CpC, cererea de consum etc.), poate fi necesară stabilirea unor măsuri CpC mai explicite și mai specifice care trebuie incluse într-un anumit tip de produs/tehnologie de informare și comunicare, în cadrul unor instrumente legislative sau nu.

55. AEPD a identificat diferite domenii (RFID, rețelele de socializare și aplicațiile de navigare) care merită, în opinia sa, în această fază o atenție deosebită din partea Comisiei și cât mai multe dintre intervențiile practice promovate mai sus. Aceste trei domenii sunt discutate pe larg în continuare.

V. **IDENTIFICAREA PRIN RADIOFRECVENȚĂ – RFID**

56. Etichetele RFID pot fi integrate în obiecte, animale și persoane. Acestea pot fi folosite pentru colectarea și stocarea unor date cu caracter personal precum fișele medicale pentru urmărirea deplasării persoanelor sau pentru realizarea profilului lor comportamental în diferite scopuri. Aceasta se poate realiza fără ca persoana să fie conștientă de acest lucru ([1]).

57. Garanțiile eficiente privind protecția datelor, confidențialitatea și toate dimensiunile etice asociate sunt esențiale pentru încrederea publică în RFID și într-un viitor internet al obiectelor. Numai atunci tehnologia poate oferi numeroasele sale beneficii economice și sociale.

V.1. **Lacunele cadrului juridic aplicabil privind protecția datelor**

58. Directiva privind protecția datelor și Directiva privind confidențialitatea în mediul electronic sunt aplicabile colectării de date prin intermediul aplicațiilor RFID ([2]). Acestea solicită, printre altele, instituirea unor garanții adecvate pentru operarea aplicațiilor RFID ([3]).

59. Cu toate acestea, cadrul juridic nu tratează în întregime toate preocupările legate de protecția datelor și confidențialitate pe care le implică utilizarea acestei tehnologii. Aceasta pentru că directivele nu sunt suficient de detaliate în ceea ce privește tipul de garanții care ar trebui puse în aplicare pentru aplicațiile RFID. Normele existente trebuie completate cu norme suplimentare care să impună garanții specifice, în special obligativitatea ca

([1]) RFID înseamnă identificare prin radiofrecvență. Principalele componente ale tehnologiei *sau* ale infrastructurii de identificare prin radiofrecvență sunt *eticheta* (adică un microcip), un cititor și o aplicație interconectată cu etichetele și cititoarele prin middleware care prelucrează datele produse. Eticheta constă într-un circuit electronic care stochează datele și o antenă care comunică datele prin unde radio. Cititorul este prevăzut cu o antenă și cu un demodulator care traduce informațiile analogice primite prin undele radio în date digitale. Apoi, informațiile pot fi transmise prin intermediul rețelelor către baze de date și servere pentru a fi procesate de un calculator.

([2]) Directiva privind confidențialitatea în mediul electronic face referire la RFID în articolul 3: „Prezenta directivă se aplică prelucrării de date personale legate de furnizarea de servicii de comunicații electronice accesibile publicului prin intermediul rețelelor de comunicații electronice din cadrul Comunității, inclusiv a rețelelor de comunicații publice care presupun colectare de date și dispozitive de identificare." Acesta este completat de considerentul 56: „Progresul tehnologic permite dezvoltarea unor noi aplicații bazate pe dispozitivele de colectare a datelor și de identificare, care pot fi dispozitive fără contact direct care utilizează frecvențele radio. De exemplu, dispozitivele de identificare prin frecvențe radio (RFID) utilizează frecvențele radio pentru a capta date numai de pe discurile identificate în mod unic, care pot fi apoi transferate de-a lungul rețelelor de comunicații existente. Larga utilizare a unor astfel de tehnologii poate să aducă beneficii economice și sociale considerabile și, astfel, să contribuie semnificativ la piața internă dacă utilizarea acestora este acceptată de către cetățeni. Pentru a se realiza acest lucru, este necesar să se garanteze că drepturile fundamentale ale persoanelor, în special dreptul la confidențialitate și la protecția datelor, sunt respectate. Atunci când astfel de dispozitive sunt conectate cu rețele de comunicații electronice accesibile publicului sau când utilizează serviciile de comunicații electronice ca infrastructură de bază, trebuie aplicate dispozițiile relevante din Directiva 2002/58/CE (Directiva asupra confidențialității și comunicațiilor electronice), inclusiv cele privind datele legate de securitate, trafic și locație și cele privind confidențialitatea."

([3]) De exemplu, articolul 17 din Directiva privind protecția datelor impune obligația de a pune în aplicare măsurile tehnice și organizatorice de protecție adecvate în vederea protejării datelor cu caracter personal împotriva distrugerii accidentale sau ilegale sau a dezvăluirii neautorizate.

tehnologia RFID să includă soluții tehnice (confidențialitate prin concepție). Acest fapt este valabil în cazul etichetelor care stochează informații personale, care ar trebui să fie prevăzute cu comenzi de întrerupere și în cazul utilizării criptografiei pentru etichetele care stochează anumite tipuri de informații personale.

V.2. **Auto-reglementarea ca prim pas**

60. În martie 2007, Comisia a adoptat o comunicare ([1]) prin care recunoștea, printre altele, necesitatea elaborării unor orientări detaliate privind aplicarea practică a RFID și oportunitatea adoptării unor criterii de proiectare în vederea evitării riscurilor pentru confidențialitate și securitate.

61. Pentru atingerea acestor obiective, Comisia a adoptat, în mai 2009, o recomandare privind aplicarea principiilor confidențialității și protecției datelor în aplicațiile bazate pe identificarea prin radiofrecvență ([2]). În aplicațiile RFID cu amănuntul, etichetele trebuie dezactivate la punctul de vânzare, exceptând făcând cazul în care persoanele și-au dat acordul. Acest fapt este valabil în cazul în care o evaluare a impactului asupra confidențialității și protecției datelor nu poate demonstra că etichetele nu reprezintă o posibilă amenințare pentru confidențialitate sau pentru protecția datelor cu caracter personal, caz în care ele ar rămâne operaționale după trecerea de punctul de vânzare, dacă persoanele nu și-au retras permisiunea în mod gratuit.

62. AEPD se declară de acord cu abordarea Comisiei de a utiliza instrumente de auto-reglementare. Cu toate acestea, așa cum este prezentat pe larg în cele ce urmează, este posibil ca auto-reglementarea să nu aducă rezultatele preconizate; în consecință, AEPD solicită Comisiei să fie pregătită să adopte măsuri alternative.

V.3. **Domenii de interes și măsurile suplimentare posibile în cazul în care auto-reglementarea nu dă rezultate**

63. AEPD este preocupată de faptul că organizațiile care utilizează aplicații RFID în sectorul comerțului cu amănuntul ar putea să nu țină seama de posibilitatea ca etichetele RFID să fie monitorizate de părți terțe nedorite. Această monitorizare ar putea dezvălui datele cu caracter personal stocate în etichetă (dacă este cazul), dar ar putea, în același timp, oferi posibilitatea unei terțe părți să urmărească sau să recunoască o persoană în timp prin simpla utilizare a identificatorilor unici conținuți de una sau mai multe etichete purtate de persoana respectivă, într-un mediu care ar putea fi chiar în afara perimetrului operațional al aplicației RFID. Un alt factor de îngrijorare pentru AEPD este faptul că operatorii aplicațiilor RFID ar putea fi tentați să se bazeze nejustificat pe excepție, lăsând astfel eticheta operațională după trecerea de punctul de vânzare.

64. Dacă se întâmplă acest lucru, ar putea fi prea târziu pentru diminuarea riscurilor pentru confidențialitate și protecția datelor persoanelor, acestea putând fi deja afectate. În plus, având în vedere natura auto-reglementării, autoritățile naționale de aplicare a legii ar putea avea o poziție de inferioritate atunci când solicită organizațiilor care utilizează aplicații RFID să aplice măsuri specifice privind confidențialitatea prin concepție.

65. Având în vedere cele de mai sus, AEPD solicită Comisiei să fie pregătită să propună instrumente legislative de reglementare a principalelor aspecte ale utilizării RFID în cazul în care punerea efectivă în aplicare a cadrului juridic existent eșuează. Evaluarea Comisiei nu ar trebui amânată în mod nejustificat; amânarea ar constitui un risc pentru persoane și ar fi contraproductivă pentru industrie, deoarece incertitudinile juridice sunt prea mari, iar remedierea unor probleme vechi este posibil să fie mai dificilă și mai costisitoare.

66. În cadrul măsurilor care ar trebui propuse, AEPD recomandă să se aibă în vedere principiul consimțământului prealabil explicit („opt-in principle") la punctul de vânzare, conform căruia toate etichetele RFID aplicate pe produsele de larg consum ar fi dezactivate în mod implicit la punctul de vânzare. Este posibil ca specificarea de către Comisie a unei tehnologii concrete care trebuie utilizată să nu fie necesară sau adecvată. În schimb, dreptul Uniunii trebuie să stabilească obligația legală de a obține consimțământul prealabil explicit, lăsându-le operatorilor libertatea de a decide modalitățile de a îndeplini această cerință.

V.4. **Alte aspecte care trebuie luate în considerare: guvernanța internetului obiectelor**

67. Informațiile furnizate de etichetele RFID – de exemplu, informațiile legate de produse – pot fi în cele din urmă interconectate într-o rețea globală a unei infrastructuri de comunicații. Aceasta este, de obicei, denumită „internetul obiectelor". Se pune problema protecției datelor/confidențialității, deoarece obiectele din lumea reală pot fi identificate prin intermediul etichetelor RFID care, pe lângă informațiile legate de produs, pot include date cu caracter personal.

68. Există numeroase întrebări deschise cu privire la autoritatea care va gestiona stocarea informațiilor legate de produsele marcate. Cum va fi organizată? Cine va avea acces la ele? În iunie 2009, Comisia a adoptat o comunicare cu privire la internetul obiectelor ([3]) care a identificat în mod explicit posibilele probleme legate de protecția datelor și confidențialitate ale acestui fenomen.

([1]) Comunicarea Comisiei din 15.3.2007 către Parlamentul European, Consiliu, Comitetul Economic și Social și Comitetul Regiunilor privind identificarea prin radiofrecvență (RFID) în Europa: etape în direcția elaborării unui cadru strategic, COM(2007) 96 final.

([2]) Recomandarea Comisiei din 12.5.2009 privind aplicarea principiilor de respectare a confidențialității și a protecției datelor în aplicațiile bazate pe identificarea prin radiofrecvență [C(2009) 3200 final].

([3]) Comunicarea Comisiei către Parlamentul European, Consiliu, Comitetul Economic și Social European și Comitetul Regiunilor privind internetul obiectelor – un plan de acțiune pentru Europa, 18.6.2009, COM(2009) 278 final.

69. AEPD ar dori să sublinieze câteva dintre aspectele puse în discuție în această comunicare, care, în opinia sa, ar trebui tratate cu atenție deosebită pe măsură ce internetul obiectelor ia amploare. În primul rând, necesitatea unei arhitecturi descentralizate ar putea facilita responsabilitatea și aplicabilitatea cadrului juridic al UE. În al doilea rând, ar trebui păstrat, în măsura posibilului, dreptul persoanelor fizice de a nu fi urmărite. Cu alte cuvinte, ar trebui să existe foarte puține cazuri de persoane urmărite prin intermediul etichetelor RFID fără consimțământul lor. Consimțământul ar trebui să fie explicit. Acest fapt este, de obicei, denumit „tăcerea cipurilor" și dreptul de a fi lăsat în pace. În ultimul rând, internetul obiectelor ar trebui conceput având în vedere principiul director al confidențialității prin concepție. De exemplu, acest lucru impune ca aplicațiile RFID concrete prevăzute cu mecanisme încorporate pentru a oferi utilizatorilor controlul să fie concepute cu setări confidențialitate prestabilite.

70. AEPD se așteaptă să fie consultată pe măsură ce Comisia pune în aplicare acțiunile prevăzute în comunicare, în special în ceea ce privește redactarea Comunicării privind confidențialitatea și încrederea într-o societate informațională ubicuă.

VI. REȚELELE DE SOCIALIZARE ȘI NECESITATEA UNOR SETĂRI DE CONFIDENȚIALITATE PRESTABILITE

71. Rețelele de socializare sunt „pe val" și par să fi depășit în popularitate e-mailul. Acestea pun în legătură persoane cu interese și/sau activități similare. Persoanele fizice își pot publica profilurile on-line și pot face schimb de fișiere media, cum ar fi filme, fotografii sau muzică, precum și profilurile profesionale.

72. Tinerii au adoptat rapid rețelele de socializare, iar această tendință continuă. În ultimii ani, vârsta medie a utilizatorilor de internet din Europa a scăzut: copii de 9-10 ani se conectează acum de câteva ori pe săptămână; cei de 12-14 ani intră on-line în fiecare zi, adesea între o oră și trei ore.

VI.1. Rețelele de socializare și cadrul juridic aplicabil privind protecția datelor și confidențialitatea

73. Dezvoltarea rețelelor de socializare le-a permis utilizatorilor să încarce pe internet informații despre ei și despre terți. În acest sens, în conformitate cu Grupul de lucru al articolului 29 ([1]), utilizatorii de internet acționează în calitate de operatori de date în sensul articolului 2 litera (d) din Directiva privind protecția datelor pentru datele pe care le încarcă ([2]). Cu toate acestea, cel mai adesea, această prelucrare se încadrează la excepția privind activitățile domestice prevăzută la articolul 3 alineatul (2) din directivă. În același timp, serviciile de socializare sunt considerate operatori de date în măsura în care asigură mijloacele de prelucrare a datelor utilizatorilor și toate serviciile de bază legate de managementul utilizatorilor (de exemplu, înregistrarea și ștergerea conturilor).

74. Din punct de vedere juridic, aceasta înseamnă că utilizatorii de internet și serviciile de socializare dețin responsabilitatea comună în ceea ce privește prelucrarea datelor cu caracter personal în calitate de „operatori de date", în sensul articolului 2 litera (d) din directivă, deși nu în aceeași măsură și având obligații diferite.

75. În consecință, utilizatorii ar trebui să știe și să înțeleagă că prin prelucrarea informațiilor lor personale și ale altora, se supun prevederilor legislației UE privind protecția datelor care impune, printre altele, obținerea consimțământului în cunoștință de cauză al persoanelor ale căror informații sunt încărcate și acordarea dreptului de rectificare, obiecție etc. persoanelor în cauză. În mod similar, serviciile de socializare trebuie, printre altele, să pună în aplicare măsuri tehnice și organizatorice adecvate, în vederea prevenirii prelucrării neautorizate, luând în considerare riscurile pe care le prezintă prelucrarea și natura datelor. Aceasta înseamnă astfel că serviciile de socializare ar trebui să asigure setări de confidențialitate prestabilite, inclusiv setări care limitează accesarea profilului la propriile contacte selectate de utilizator. Setările ar trebui, de asemenea, să necesite consimțământul utilizatorului înainte ca un profil să devină accesibil unor părți terțe, iar profilurile al căror acces este restricționat nu ar trebui să poată fi găsite prin utilizarea unor motoare de căutare interne.

76. Din păcate, există o diferență între cerințele legale și respectarea lor efectivă. În timp ce, din punct de vedere juridic, utilizatorii de internet sunt considerați operatori de date și trebuie să se supună cadrului juridic UE privind protecția datelor și confidențialitatea, în realitate, aceștia nu sunt de multe ori conștienți de acest rol. În termeni generali, aceștia nu înțeleg că prelucrează date cu caracter personal și că publicarea acestor informații implică riscuri pentru confidențialitate și protecția datelor. Tinerii, în special, publică on-line informații subestimând consecințele pentru ei și pentru alții, de exemplu, în contextul înscrierii ulterioare în cadrul unor instituții de învățământ sau al depunerii candidaturii pentru anumite posturi.

([1]) A se vedea Avizul nr. 163, 5/2009 al Grupului de lucru al articolului 29 privind rețelele de socializare on-line, adoptat la 12 iunie 2009.

([2]) „Operator" înseamnă persoana fizică sau juridică, autoritatea publică, agenția sau orice alt organism care, singur sau împreună cu altele, stabilește scopurile și mijloacele de prelucrare a datelor cu caracter personal; atunci când scopurile și mijloacele prelucrării sunt stabilite prin acte cu putere de lege sau norme administrative interne sau comunitare, operatorul sau criteriile specifice pentru desemnarea acestuia pot fi stabilite prin dreptul intern sau comunitar.

77. În același timp, furnizorii de rețele de socializare preselectează adesea setările implicite pe baza opțiunilor de neparticipare, facilitând astfel dezvăluirea informațiilor personale. Unele setări permit vizualizarea implicită a profilurilor prin intermediul unor motoare de căutare obișnuite. Ne punem astfel întrebarea dacă persoanele și-au dat, într-adevăr, consimțământul în ceea ce privește divulgarea acestor informații și dacă rețelele de socializare respectă articolul 17 din directivă (descris mai sus), care îi obligă să pună în aplicare măsuri tehnice și organizatorice adecvate pentru prevenirea prelucrării neautorizate.

VI.2. **Riscurile generate de rețelele de socializare și acțiunile sugerate în vederea abordării lor**

78. Din cele prezentate mai sus rezultă o creștere a riscului asupra confidențialității și protecției datelor unei persoane. Utilizatorii de internet și cei ale căror date au fost încărcate pe internet sunt expuși unor încălcări flagrante ale confidențialității și ale protecției datelor.

79. În acest context, Comisia ar trebui să analizeze măsurile care trebuie și pot fi adoptate pentru remedierea acestei situații. Acest aviz nu oferă un răspuns cuprinzător la această problemă, ci prezintă o serie de sugestii în vederea analizării ulterioare.

Investirea în educarea utilizatorilor de internet

80. Prima sugestie se referă la investirea în educarea utilizatorilor. În acest sens, instituțiile UE și autoritățile naționale ar trebui să investească în educarea și creșterea gradului de conștientizare în ceea ce privește amenințările pe care le prezintă site-urile rețelelor de socializare. De exemplu, DG Societatea Informațională și Media administrează Programul pentru un internet mai sigur, menit să responsabilizeze și să protejeze copiii și tinerii, de exemplu, prin activitățile de sensibilizare ([1]). De curând, instituțiile UE au lansat campania „Gândește-te înainte să postezi” („Think before you post”) cu scopul de a crește gradul de conștientizare a riscurilor pe care le implică dezvăluirea informațiilor personale unor străini.

81. AEPD încurajează Comisia să sprijine în continuare acest tip de activitate. Totuși, și furnizorii de rețele de socializare ar trebui să joace un rol activ în acest sens, având în vedere că au o responsabilitate legală și socială în ceea ce privește educarea utilizatorilor cu privire la modul de utilizare a serviciilor lor în mod sigur și cu respectarea confidențialității.

82. Astfel cum se descrie mai sus, atunci când se postează informații pe rețelele de socializare, acestea pot fi disponibile implicit prin diverse alte moduri. De exemplu, informațiile pot fi disponibile publicului larg, inclusiv motoarelor de căutare, care le pot repertoriza și furniza astfel link-uri directe către ele. Pe de altă parte, informațiile pot fi limitate doar la „prieteni selectați” sau pot fi complet confidențiale. Evident, permisiunea de a accesa profilul și terminologia utilizată pot varia de la un site la altul.

83. Cu toate acestea, așa cum s-a subliniat mai sus, foarte puțini utilizatori ai serviciilor de socializare știu cum să controleze accesul la informațiile pe care le postează, ca să nu mai vorbim de modul în care pot fi modificate setările de confidențialitate prestabilite. Setările de confidențialitate rămân, de obicei, neschimbate deoarece utilizatorii nu cunosc implicațiile nemodificării lor sau nu știu cum să facă acest lucru. Astfel, cel mai adesea, nemodificarea setărilor de confidențialitate nu înseamnă că persoanele fizice au luat o decizie în cunoștință de cauză atunci când au acceptat să își publice informațiile. În acest context, este deosebit de important ca părțile terțe, cum ar fi motoarele de căutare, să nu ofere link-uri către profiluri individuale, presupunând că utilizatorii și-au dat implicit consimțământul (având în vedere că nu și-au modificat setările de confidențialitate) ca informațiile lor să fie puse la dispoziție fără restricții.

84. Deși educarea utilizatorilor poate ajuta la remedierea acestei situații, nu poate funcționa singură. Așa cum recomandă Grupul de lucru al articolului 29 în avizul său privind rețelele de socializare, furnizorii de rețele de socializare ar trebui să ofere setări de confidențialitate implicite gratuite. Astfel, utilizatorii ar conștientiza mai bine acțiunile lor și ar putea să ia decizii mai bune legate de măsura în care doresc să ofere informații și cui.

Rolul auto-reglementării

85. Comisia a încheiat un acord cu 20 de furnizori de rețele de socializare, cunoscut sub denumirea de „Principii pentru rețele de socializare mai sigure în UE” ([2]). Obiectivul acordului îl reprezintă îmbunătățirea siguranței minorilor atunci când utilizează site-urile de socializare din Europa. Aceste principii includ multe dintre cerințele rezultate din aplicarea cadrului juridic privind protecția datelor descris mai sus, de exemplu, condiția de a pune la dispoziția utilizatorilor instrumente și tehnologie pentru a asigura posibilitatea acestora de a controla utilizarea și difuzarea informațiilor lor personale. Acordul include, de asemenea, necesitatea de a asigura setări de confidențialitate prestabilite.

86. La începutul lunii ianuarie 2010, Comisia a făcut cunoscute concluziile unui raport de evaluare a punerii în aplicare a principiilor ([3]). AEPD este preocupată de faptul că acest raport arată că au fost adoptate prea puține măsuri. De exemplu, raportul a constatat

([1]) Informații cu privire la acest program sunt disponibile la: http://ec.europa.eu/information_society/activities/sip/index_en.htm

([2]) Principiile sunt disponibile la: http://ec.europa.eu/information_society/activities/social_networking/docs/sn_principles.pdf

([3]) Raport privind evaluarea aplicării principiilor pentru rețele de socializare mai sigure în UE, disponibil la: http://ec.europa.eu/information_society/activities/social_networking/docs/final_report/first_part.pdf

probleme legate de comunicarea măsurilor și instrumentelor de securitate disponibile pe site-uri. De asemenea, a constatat că mai puțin de jumătate dintre semnatarii acordului limitează accesul la profilurile minorilor numai la prietenii acestora.

Necesitatea unor setări de confidențialitate prestabilite obligatorii

87. În acest context, problema-cheie o reprezintă necesitatea adoptării unor măsuri politice suplimentare pentru a garanta că serviciile rețelelor de socializare includ setări de confidențialitate prestabilite. Această chestiune a fost pusă în discuție de fostul comisar pentru societatea informațională Viviane Reding, care a subliniat că adoptarea unei legislații în acest sens poate fi necesară ([1]). În aceeași ordine de idei, Comitetul Economic și Social European a afirmat că, pe lângă auto-reglementare, legea ar trebui să impună standarde minime de protecție ([2]).

88. Așa cum s-a arătat mai sus, obligația furnizorilor de rețele de socializare de a pune în aplicare setări de confidențialitate prestabilite poate rezulta indirect din articolul 17 al Directivei privind protecția datelor ([3]), care îi obligă pe operatorii de date să ia măsurile tehnice și organizatorice adecvate („atât în momentul proiectării sistemului de prelucrare, cât și în cel al prelucrării în sine"), pentru a menține securitatea și a preveni prelucrarea neautorizată, ținând seama de riscurile reprezentate de prelucrare și de natura datelor.

89. Cu toate acestea, acest articol este mult prea general și, în acest context, nu are un caracter specific. Acesta nu precizează în mod clar ce se înțelege prin măsuri tehnice și organizatorice adecvate în contextul rețelelor de socializare. Astfel, situația actuală este una de insecuritate juridică, care cauzează probleme atât autorităților de reglementare, cât și persoanelor fizice, a căror confidențialitate și ale căror date personale nu sunt complet protejate.

90. Având în vedere cele de mai sus, AEPD solicită Comisiei să elaboreze o legislație care să includă, cel puțin, obligația generală de utilizare a setărilor de confidențialitate, alături de alte cerințe mai exacte:

(a) să prevadă setări care să limiteze accesul la profilurile utilizatorilor la propriile contacte auto-selectate. Setările ar trebui, de asemenea, să necesite consimțământul utilizatorului înainte ca profilul său să fie accesibil unor părți terțe;

(b) să prevadă ca profilurile cu acces restricționat să nu poată fi descoperite prin utilizarea unor motoare de căutare interne/externe.

91. Pe lângă prevederea unor setări de confidențialitate prestabilite obligatorii, rămâne întrebarea dacă ar fi adecvat să se adopte unele măsuri specifice suplimentare privind protecția datelor și alte măsuri (de exemplu, legate de protecția minorilor). Se pune astfel problema mai generală dacă ar fi adecvat să se creeze un cadru specific pentru aceste tipuri de servicii, care, pe lângă prevederea unor setări de confidențialitate obligatorii, ar reglementa și alte aspecte. AEPD solicită Comisiei să ia în considerare această problemă.

VII. **SETĂRI DE CONFIDENȚIALITATE PRESTABILITE ALE BROWSERULUI PENTRU GARANTAREA CONSIMȚĂMÂNTULUI ÎN CUNOȘTINȚĂ DE CAUZĂ ÎN CEEA CE PRIVEȘTE PRIMIREA DE MATERIALE PUBLICITARE**

92. Furnizorii de rețele publicitare utilizează module cookie și alte dispozitive pentru a urmări comportamentul utilizatorilor individuali când navighează pe internet, în vederea catalogării intereselor acestora și a realizării profilurilor lor. Aceste informații sunt apoi utilizate pentru a le trimite mesaje publicitare adecvate ([4]).

VII.1. **Problemele și riscurile rămase în cadrul juridic existent privind protecția datelor/confidențialitatea**

93. Această prelucrare este tratată în Directiva privind protecția datelor (atunci când este vorba de date cu caracter personal) și în articolul 5 alineatul (3) din Directiva privind confidențialitatea în mediul electronic. Acest articol prevede în mod explicit ca utilizatorul să fie informat și să aibă posibilitatea de a reacționa, acceptând sau refuzând stocarea dispozitivelor precum module cookie etc. pe calculatorul său sau pe alt dispozitiv ([5]).

94. Până în prezent, furnizorii de rețele publicitare s-au bazat pe setările browserului și pe politicile de confidențialitate pentru a informa utilizatorii și a le acorda posibilitatea de a accepta sau de a refuza modulele cookie. Aceștia au

([1]) Viviane Reding, Membru al Comisiei Europene, responsabil pentru programul DG Societatea Informațională și Media „Gândește-te înainte să postezi! Cum să facem site-urile de socializare mai sigure pentru copii și adolescenți". Ziua pentru un internet mai sigur, Strasbourg, 9 februarie 2010.

([2]) Avizul Comitetului Economic și Social European privind impactul site-urilor de socializare asupra cetățenilor/consumatorilor, 4 noiembrie 2009.

([3]) Fapt dezvoltat și la punctul 33 din prezentul document.

([4]) Modulele cookie de urmărire sunt mici fișiere de text care conțin un singur identificator. De regulă, furnizorii de rețele publicitare (precum și operatorii sau editorii site-urilor web) plasează module cookie pe hard disk-ul vizitatorilor, în special în browserul utilizatorilor de internet, atunci când utilizatorii accesează prima dată site-urile web pe care apar mesaje publicitare ca parte din rețea. Utilizarea modulelor cookie permite furnizorului de rețele publicitare să recunoască un fost vizitator care se întoarce la acel site sau care vizitează orice site web care este partener în cadrul acelei rețele publicitare. Aceste vizite repetate permit furnizorului de publicitate să realizeze un profil al vizitatorului.

([5]) Articolul 5 alineatul (3) din Directiva privind confidențialitatea în mediul electronic a fost recent modificat, pentru a consolida protecția împotriva interceptării comunicațiilor utilizatorilor prin utilizarea – de exemplu – a spyware-ului și a modulelor cookie stocate pe calculatorul unui utilizator sau pe alt dispozitiv. Conform noii directive, utilizatorilor ar trebui să li se ofere informații mai pertinente și să le fie puse la dispoziție metode mai simple de a controla dacă doresc sau nu stocarea de module cookie pe echipamentele lor terminale.

explicat în politicile de confidențialitate ale editorilor cum se poate renunța la primirea de module cookie sau cum se pot accepta acestea în funcție de caz. În acest sens, aceștia au intenționat să își respecte obligația de a le oferi utilizatorilor dreptul de a refuza modulele cookie.

95. Deși, teoretic, această metodă (prin intermediul browserului) ar putea, într-adevăr, să asigure un consimțământ semnificativ în cunoștință de cauză, în realitate, nu este deloc așa. În general, utilizatorii nu înțeleg colectarea de date, cu atât mai puțin de către părți terțe, importanța acestor date, scopul lor, modul în care funcționează tehnologia și, în mod special, cum și în ce situații să-și retragă permisiunea. Măsurile pe care utilizatorii trebuie să le ia pentru a-și retrage permisiunea par nu numai complicate, ci și excesive (mai întâi, aceștia trebuie să își seteze browserul pentru a accepta module cookie, apoi să folosească opțiunea de neparticipare).

96. Prin urmare, practic, foarte puține persoane folosesc opțiunea de neparticipare, nu pentru că au luat decizia în cunoștință de cauză de a accepta publicitatea comportamentală, ci, mai degrabă, pentru că nu își dau seama că nefolosind opțiunea de neparticipare, își exprimă de fapt acceptul.

97. În consecință, deși din punct de vedere juridic, articolul 5 alineatul (3) din Directiva privind confidențialitatea în mediul electronic prevede o protecție juridică eficientă, practic, se consideră că utilizatorii de internet sunt de acord să fie monitorizați în vederea primirii de materiale de publicitate comportamentală când, de fapt, în numeroase cazuri, dacă nu în majoritatea cazurilor, aceștia nu sunt deloc conștienți de această monitorizare.

98. Grupul de lucru al articolului 29 pregătește un aviz binevenit menit să clarifice condițiile legale pe care le implică publicitatea comportamentală. Cu toate acestea, interpretarea în sine ar putea să nu fie suficientă pentru soluționarea acestei situații și ar putea fi nevoie ca Uniunea Europeană să ia măsuri suplimentare.

VII.2. **Necesitatea unor acțiuni suplimentare, în special prevederea setărilor de confidențialitate prestabilite obligatorii**

99. Așa cum s-a prezentat mai sus, browserele web permit, de regulă, un anumit grad de control asupra anumitor tipuri de module cookie. În prezent, setările prestabilite ale majorității browserelor web acceptă toate modulele cookie. Cu alte cuvinte, browserele sunt presetate să accepte toate modulele cookie, indiferent de scopul acelui modul. Numai în cazul în care utilizatorul modifică setările aplicației sale de navigare pentru a refuza modulele cookie, ceea ce, așa cum s-a menționat mai sus, foarte puțin utilizatori fac, acesta nu va primi module cookie. Mai mult, nu există niciun expert de confidențialitate la prima instalare sau la actualizarea aplicațiilor de navigare.

100. O modalitate de reducere a consecințelor problemei de mai sus ar fi cazul în care browserele ar fi prevăzute cu setări de confidențialitate prestabilite. Cu alte cuvinte, dacă ar fi prevăzute cu setarea „neacceptarea modulelor cookie terțe". În completarea acestei prevederi și pentru a-i spori eficiența, browserele ar trebui să solicite utilizatorilor să parcurgă un expert de confidențialitate atunci când instalează pentru prima dată sau actualizează browserul. Este nevoie de o mai mare varietate și de informații clare privind tipurile de module cookie și utilitatea unora dintre ele. Utilizatorii care doresc să fie monitorizați cu scopul de a primi mesaje publicitare vor fi informați corespunzător și vor trebui să modifice setările browserului. Astfel, aceștia vor avea control sporit asupra datelor lor personale și confidențialității. În opinia AEPD, aceasta ar fi o modalitate eficientă de respectare și de păstrare a consimțământului utilizatorilor ([1]).

101. Ținând seama, pe de o parte, de amploarea problemei, cu alte cuvinte, de numărul de utilizatori de internet care sunt în prezent monitorizați pe baza unui consimțământ ireal și, pe de altă parte, de importanța interesului pus în joc, necesitatea adoptării unor măsuri suplimentare de siguranță devine și mai stringentă. Punerea în aplicare a principiului CpC în aplicațiile de navigare pe internet ar putea face o diferență clară în ceea ce privește controlul persoanelor fizice asupra practicilor de colectare a datelor utilizate în scopuri publicitare.

102. Din aceste motive, AEPD solicită Comisiei să ia în considerare luarea unor măsuri legislative care să impună utilizarea în browsere a unor setări de confidențialitate prestabilite obligatorii și furnizarea informațiilor relevante.

VIII. **ALTE PRINCIPII MENITE SĂ PROTEJEZE CONFIDENȚIALITATEA/DATELE PERSONALE ALE PERSOANELOR FIZICE**

103. Deși principiul CpC poate îmbunătăți în mare măsură protecția datelor cu caracter personal și confidențialității persoanelor fizice, se impune conceperea și punerea în aplicare în legislație a unor principii complementare pentru a asigura încrederea consumatorilor în TIC. În acest context, AEPD abordează principiul responsabilității și finalizarea unui cadru obligatoriu de încălcare a securității, aplicabil în toate sectoarele.

VIII.1. **Principiul responsabilității, pentru asigurarea respectării principiului confidențialității prin concepție**

104. Documentul Grupului de lucru al articolului 29 intitulat „Viitorul confidențialității" ([2]) a recomandat includerea principiului responsabilității în Directiva privind protecția datelor. Acest principiu, recunoscut într-o serie de

([1]) În același timp, AEPD este conștientă de faptul că aceasta nu rezolvă complet problema, în măsura în care există module cookie care nu pot fi controlate prin intermediul browserului, cum ar fi așa-numitele module flash cookie. În acest caz, dezvoltatorii de browsere ar trebui, la lansarea de noi browsere, să integreze implicit sisteme de control flash în sistemele de control a modulelor cookie.

([2]) Avizul nr. 168 al Grupului de lucru al articolului 29 privind viitorul confidențialității, contribuție comună la Consultarea Comisiei Europene privind cadrul juridic al dreptului fundamental la protecția datelor cu caracter personal, adoptat la 1 decembrie 2009.

instrumente multinaționale privind protecția datelor ([1]), impune organizațiilor să pună în aplicare procedee în vederea respectării legislației existente și să instituie metode de evaluare și de demonstrare a conformității cu legislația și alte instrumente obligatorii.

105. AEPD susține pe deplin recomandarea Grupului de lucru al articolului 29. Aceasta consideră că principiul va fi extrem de relevant în ceea ce privește promovarea aplicării efective a principiilor și obligațiilor privind protecția datelor. Responsabilitatea va impune operatorilor de date să demonstreze că au instituit mecanismul necesar în vederea respectării legislației aplicabile privind protecția datelor. Aceasta va contribui la punerea efectivă în aplicare a principiului confidențialității prin concepție în tehnologiile TIC, fiind un element deosebit de adecvat pentru demonstrarea responsabilității.

106. Pentru a măsura și demonstra responsabilitatea, operatorii de date ar putea utiliza proceduri interne și părți terțe care pot efectua audituri sau alte tipuri de controale și verificări și care pot acorda, prin urmare, sigilii sau premii. În acest context, AEPD solicită Comisiei să analizeze dacă, pe lângă principiul general al responsabilității, ar putea fi de ajutor să se solicite prin lege instituirea unor măsuri specifice de responsabilizare, precum necesitatea de a realiza evaluări ale impactului asupra confidențialității și protecției datelor, și în ce condiții.

VIII.2. **Încălcarea securității: finalizarea cadrului juridic**

107. Modificările aduse anul trecut Directivei privind confidențialitatea în mediul electronic au introdus necesitatea de notificare a cazurilor de încălcare a securității datelor persoanelor în cauză și autorităților competente. Încălcarea securității datelor este, în general, definită ca fiind orice încălcare ce duce la distrugerea, pierderea, dezvăluirea etc. datelor cu caracter personal transmise, stocate sau altfel prelucrate în legătură cu serviciul. Notificarea persoanelor va fi necesară dacă există probabilitatea ca încălcarea securității datelor să aibă un impact negativ asupra datelor lor personale și confidențialității. Acest lucru este valabil, de exemplu, în cazul în care încălcarea ar putea duce la furtul de identitate, la o umilire majoră sau la distrugerea reputației. Notificarea autorităților competente va fi necesară în cazul oricărei încălcări a securității datelor, indiferent dacă există sau nu un risc pentru persoanele fizice.

Aplicarea obligațiilor privind încălcarea securității în toate sectoarele

108. Din păcate, această obligație se aplică numai în cazul furnizorilor de servicii de comunicații electronice publice, precum companiile de telefonie, furnizorii de internet, furnizorii de mail web etc. AEPD solicită Comisiei să prezinte propuneri privind încălcarea securității cu aplicabilitate în toate sectoarele. În ceea ce privește conținutul acestui cadru, AEPD consideră cadrul juridic privind încălcarea securității, adoptat în Directiva privind confidențialitatea în mediul electronic, ca asigurând un echilibru adecvat între protecția drepturilor persoanelor fizice, inclusiv drepturile lor la date cu caracter personal și confidențialitate, și obligațiile impuse entităților în cauză. În același timp, este vorba de un cadru incisiv, având în vedere că este susținut de dispoziții de executare importante, care asigură autorităților competențe suficiente de investigare și de sancționare în cazul nerespectării acestora.

109. În consecință, AEPD solicită Comisiei să adopte o propunere legislativă de aplicare a acestui cadru în toate sectoarele, cu adaptările necesare, dacă este cazul. În plus, astfel s-ar asigura aplicarea acelorași standarde și proceduri în toate sectoarele.

Finalizarea cadrului juridic inclus în Directiva privind confidențialitatea în mediul electronic prin comitologie

110. Directiva revizuită privind confidențialitatea în mediul electronic împuternicește Comisia să adopte măsuri tehnice de punere în aplicare, și anume, măsuri detaliate privind notificarea încălcării securității, printr-o procedură de comitologie ([2]). Această împuternicire este justificată pentru a asigura punerea în aplicare coerentă a cadrului juridic privind încălcarea securității. Punerea coerentă în aplicare urmărește ca persoanele din Comunitate să se bucure de un nivel echivalent de protecție și ca entitățile în cauză să nu fie împovărate cu cerințe divergente privind notificarea.

111. Directiva privind confidențialitatea în mediul electronic a fost adoptată în noiembrie 2009. Nu pare să existe niciun motiv care să justifice amânarea adoptării măsurilor tehnice privind punerea în aplicare. AEPD a organizat două seminarii care au urmărit schimbul și acumularea de experiență privind notificarea încălcării securității datelor. AEPD este pregătită să facă rezultatele acestui exercițiu cunoscute și așteaptă cu nerăbdare să colaboreze cu Comisia și cu alte părți interesate în vederea perfecționării cadrului juridic global privind încălcarea securității datelor.

112. AEPD solicită Comisiei să ia măsurile necesare într-un timp cât mai scurt. Înainte să adopte măsurile tehnice de punere în aplicare, Comisia trebuie să demareze un vast proces de consultări, în care vor fi consultate ENISA, AEPD și Grupul de lucru al articolului 29. Mai mult, procesul de consultare trebuie să includă și alte părți interesate competente, în special în vederea comunicării celor mai bune mijloace tehnice și economice disponibile de punere în aplicare.

([1]) Orientările OCDE din 1980 privind protecția confidențialității și fluxurile transfrontaliere de date cu caracter personal; Declarația de confidențialitate de la Madrid privind standardele globale de confidențialitate pentru o lume globală, 3 noiembrie 2009.

([2]) Comitologia implică adoptarea de măsuri tehnice de punere în aplicare printr-un comitet de reprezentanți ai statelor membre prezidat de Comisie. În ceea ce privește Directiva privind confidențialitatea în mediul electronic, se aplică așa-numita procedură de reglementare cu control, ceea ce înseamnă că Parlamentul European și Consiliul se pot opune măsurilor propuse de Comisie. A se vedea http://europa.eu/scadplus/glossary/comitology_en.htm

IX. **CONCLUZII**

113. Încrederea sau, mai degrabă, lipsa încrederii, a fost identificată drept o problemă esențială în ceea ce privește introducerea și dezvoltarea cu succes a tehnologiilor informațiilor și comunicațiilor. Dacă oamenii nu au încredere în TIC, aceste tehnologii au șanse mici de reușită. Încrederea în TIC depinde de diferiți factori; asigurarea faptului că aceste tehnologii nu erodează drepturile fundamentale ale individului la confidențialitate și la protecția datelor reprezintă un aspect esențial.

114. Pentru a consolida și mai mult cadrul juridic privind protecția datelor/confidențialitatea, ale cărui principii rămân complet valabile în societatea informațională, AEPD propune Comisiei să includă principiul confidențialității prin concepție la diferite niveluri de legislație și în procesul de elaborare a politicilor.

115. Aceasta recomandă Comisiei să urmeze 4 planuri de acțiune:

(a) să propună includerea unei prevederi generale cu privire la principiul confidențialității prin concepție în cadrul juridic privind protecția datelor. Această prevedere ar trebui să fie neutră din punct de vedere tehnologic, iar respectarea sa obligatorie, la diferite etape;

(b) să dezvolte această prevedere generală în prevederi specifice, atunci când sunt propuse instrumente juridice specifice în diferite sectoare. Este posibil ca aceste prevederi specifice să fie deja incluse în instrumente juridice, în temeiul articolului 17 al Directivei privind protecția datelor (și a altor legi existente);

(c) să includă principiul CpC ca principiu director în Agenda digitală europeană;

(d) să introducă principiul CpC în alte inițiative ale UE (în special nelegislative).

116. În trei domenii TIC desemnate, AEPD recomandă Comisiei să evalueze necesitatea de a prezenta propuneri de punere în aplicare a principiului confidențialității prin concepție în moduri specifice:

(a) în ceea ce privește RFID, să propună măsuri legislative care să reglementeze principalele chestiuni legate de utilizarea RFID, în cazul în care punerea efectivă în aplicare a cadrului juridic existent prin auto-reglementare eșuează. În special, să prevadă principiul consimțământului prealabil explicit la punctul de vânzare, conform căruia toate etichetele RFID aplicate pe produsele de larg consum sunt dezactivate în mod implicit la punctul de vânzare;

(b) în ceea ce privește rețelele de socializare, să elaboreze o legislație care să includă, cel puțin, obligația generală de utilizare a setărilor de confidențialitate, alături de alte cerințe mai precise privind limitarea accesului la profilurile utilizatorului la propriile contacte autoselectate și care să asigure că profilurile cu acces restricționat nu pot fi descoperite prin utilizarea unor motoare de căutare interne/externe;

(c) în ceea ce privește mesajele publicitare orientate, să aibă în vedere elaborarea unei legislații care să autorizeze setări ale browserelor care să respingă implicit acele module cookie terțe și care să le solicite utilizatorilor să parcurgă un expert de confidențialitate atunci când instalează pentru prima dată sau își actualizează browserul.

117. În ultimul rând, AEPD recomandă Comisiei:

(a) să aibă în vedere punerea în aplicare a principiului responsabilității în directiva existentă privind protecția datelor; și

(b) să dezvolte un cadru de norme și proceduri de punere în aplicare a prevederilor referitoare la notificarea încălcării securității, prevăzute în directiva asupra confidențialității și comunicațiilor electronice, și să le extindă aplicabilitatea la toți operatorii de date.

Adoptat la Bruxelles, 18 martie 2010.

Peter HUSTINX

Autoritatea Europeană pentru Protecția Datelor