I

(Rezoluții, recomandări și avize)

AVIZE

AUTORITATEA EUROPEANĂ PENTRU PROTECȚIA DATELOR

Avizul Autorității Europene pentru Protecția Datelor privind propunerea de directivă a Parlamentului European și a Consiliului de modificare, printre altele, a Directivei 2002/58/CE privind prelucrarea datelor personale și protejarea confidențialității în sectorul comunicațiilor publice (Directiva asupra confidențialității și comunicațiilor electronice)

(2008/C 181/01)

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 ([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 publice ([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, și, în special, articolul 41 al acestuia ([3]),

având în vedere solicitarea de aviz primită la 16 noiembrie 2007 din partea Comisiei Europene, în conformitate cu articolul 28 alineatul (2) din Regulamentul (CE) nr. 45/2001,

ADOPTĂ PREZENTA DECIZIE:

I. **INTRODUCERE**

1. La 13 noiembrie 2007, Comisia a adoptat o propunere de directivă de modificare, printre altele, a Directivei 2002/58/CE privind prelucrarea datelor personale și protejarea confidențialității în sectorul comunicațiilor publice (denumită în continuare „propunerea” sau „modificările propuse”). Versiunea actuală a Directivei 2002/58/CE este denumită în general, precum și în cadrul prezentului aviz, „Directiva privind confidențialitatea în mediul electronic”.

([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.

2. Propunerea urmărește să consolideze gradul de protecție a confidențialității și a datelor personale în sectorul comunicațiilor electronice. Acest obiectiv nu se realizează prin reformularea completă a directivei existente, ci, mai degrabă, propunând modificări *ad hoc*, care să urmărească, în principal, consolidarea dispozițiilor privind securitatea și îmbunătățirea mecanismelor de punere în aplicare.

3. Propunerea face parte dintr-o reformă mai amplă a celor cinci directive privind telecomunicațiile („pachetul telecomunicații"). Pe lângă propunerile de revizuire a pachetului telecomunicații ([1]), Comisia a adoptat, în același timp, și o propunere de regulament de instituire a Autorității europene de reglementare a pieței comunicațiilor electronice ([2]).

4. Observațiile incluse în prezentul aviz se limitează la modificările propuse la Directiva privind confidențialitatea în mediul electronic, cu excepția cazul în care acestea din urmă au la bază concepte sau dispoziții cuprinse în propunerile de revizuire a pachetului telecomunicații. În plus, anumite comentarii cuprinse în prezentul aviz se referă la unele dispoziții ale Directivei privind confidențialitatea în mediul electronic care nu au fost modificate prin propunere.

5. Prezentul aviz abordează următoarele teme: (i) domeniul de aplicare a Directivei privind confidențialitatea în mediul electronic, în special serviciile implicate [modificare propusă la articolul 3 alineatul (1)]; (ii) notificarea încălcărilor securității [modificare propusă prin care se introduc articolul 4 alineatele (3) și (4)]; (iii) dispozițiile privind „cookies", „spyware" și alte instrumente similare [modificare propusă la articolul 5 alineatul (3)]; (iv) acțiunile legale întreprinse de furnizorii de servicii de comunicații electronice și de alte persoane juridice [modificare propusă prin care se introduce articolului 13 alineatul (6)] și (v) consolidarea dispozițiilor de punere în aplicare (modificare propusă prin care se introduce articolului 15a).

Consultarea Autorității Europene pentru Protecția Datelor și consultarea publică mai amplă

6. Comisia a înaintat propunerea AEPD la 16 noiembrie 2007. AEPD consideră această comunicare drept o solicitare de a consilia instituțiile și organismele comunitare, astfel cum se prevede la articolul 28 alineatul (2) din Regulamentul (CE) nr. 45/2001 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 [denumit în continuare „Regulamentul (CE) nr. 45/2001"].

7. Înaintea adoptării propunerii, Comisia a consultat în mod informal AEPD cu privire la proiectul de propunere. AEPD a apreciat această inițiativă, deoarece i-a oferit ocazia de a face anumite sugestii pe marginea proiectului de propunere înaintea adoptării acesteia de către Comisie. AEPD constată cu satisfacție faptul că unele dintre sugestiile sale se reflectă în propunere.

8. Adoptarea propunerii a fost precedată de o consultare publică amplă, o practică apreciată de AEPD. Într-adevăr, în iunie 2006, Comisia a lansat o consultare publică cu privire la Comunicarea sa privind revizuirea pachetului telecomunicații, în cadrul căreia și-a prezentat opiniile cu privire la situație și a înaintat câteva propuneri de modificare ([3]). Grupul de lucru pentru protecția datelor „articolul 29" („GL 29") printre ai cărui membrii se numără și AEPD, a profitat de această ocazie pentru a-și prezenta opiniile cu privire la modificările propuse, sub forma unui aviz adoptat la 26 septembrie 2006 ([4]).

([1]) Modificările propuse la directivele privind telecomunicațiile sunt prezentate în următoarele propuneri: (i) Propunerea de directivă a Parlamentului European și a Consiliului de modificare a Directivelor Parlamentului European și ale Consiliului 2002/21/CE privind un cadru de reglementare comun pentru rețelele și serviciile de comunicații electronice, 2002/19/CE privind accesul la rețelele de comunicații electronice și la infrastructura asociată, precum și interconectarea acestora și 2002/20/CE privind autorizarea rețelelor și serviciilor de comunicații electronice, 13 noiembrie 2007, COM(2007) 697 final; (ii) Propunerea de directivă a Parlamentului European și a Consiliului de modificare a Directivei 2002/22/CE privind serviciul universal și drepturile utilizatorilor cu privire la rețelele și serviciile electronice de comunicații, a Directivei 2002/58/CE 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, 13 noiembrie 2007, COM(2007) 698 final.

([2]) Propunerea de regulament al Parlamentului European și al Consiliului de instituire a Autorității europene de reglementare a piețelor comunicațiilor electronice, 13 noiembrie 2007, COM(2007) 699 final.

([3]) Comunicarea privind cadrul de reglementare al UE pentru rețele și servicii de comunicații electronice [SEC(2006) 816] adoptată la 29 iunie 2006. Comunicare a fost completată de un document de lucru al serviciilor Comisiei [COM(2006) 334 final].

([4]) Avizul 8/2006 privind revizuirea cadrului de reglementare pentru comunicațiile și serviciile electronice, cu accentul pe Directiva privind confidențialitatea în mediul electronic adoptată la 26 septembrie 2006.

Opiniile cu caracter general ale AEPD

9. În general, opiniile AEPD cu privire la propunere sunt favorabile. AEPD sprijină pe deplin obiectivele urmărite de Comisie prin adoptarea unei propuneri de consolidare a gradului de protecție a confidențialității și a datelor personale în sectorul comunicațiilor electronice. AEPD salută, în special, adoptarea unui sistem de notificare obligatorie privind încălcarea securității [modificare la articolul 4 din Directiva privind confidențialitatea în mediul electronic, prin care se introduc alineatele (3) și (4)]. Atunci când au loc încălcări ale securității datelor, notificarea prezintă avantaje evidente, deoarece sporește responsabilitate organizațiilor, determină societățile să pună în aplicare măsuri de securitate stricte și permite identificarea celor mai fiabile tehnologii în domeniul protecției informațiilor. În plus, aceasta permite persoanelor afectate să ia măsuri pentru a se proteja împotriva furtului de identitate sau împotriva altor utilizări necorespunzătoare ale informațiilor lor personale.

10. AEPD salută alte modificări cuprinse în propunere, precum posibilitatea persoanelor juridice cu interese legitime de a acționa în justiție persoanele care încalcă anumite dispoziții ale Directivei privind confidențialitatea în mediul electronic [modificare la articolul 13, prin care se introduce alineatul (6)]. Este de asemenea apreciată consolidarea competențelor de investigare ale autorităților naționale de reglementare, deoarece le va permite acestora să evalueze dacă prelucrarea datelor se desfășoară în conformitate cu legislația și să identifice contravenienții [completare la articolul 15a alineatul (3)]. Posibilitatea de a stopa cât mai curând cu putință prelucrarea ilegală a datelor personale și încălcarea confidențialității este o măsură necesară pentru a proteja drepturile și libertățile persoanelor. În acest scop, articolul 15a alineatul (2) propus, care recunoaște competența autorităților naționale de reglementare de a ordona încetarea încălcărilor este binevenit, deoarece le va permite acestora să stopeze imediat prelucrarea ilegală gravă.

11. Abordarea propunerii și majoritatea modificărilor propuse sunt conforme cu opiniile privind o politică viitoare de protecție a datelor, prezentate în avizele precedente ale AEPD, cum ar fi Avizul privind punerea în aplicare a Directivei privind protecția datelor ([1]). Printre altele, abordarea se bazează pe convingerea că, cu toate că nu sunt necesare principii noi de protecție a datelor, este nevoie de mai multe norme specifice pentru a aborda aspectele privind protecția datelor pe care le ridică noile tehnologii, cum ar fi internetul, RFID, etc., precum și de instrumente care să contribuie la consolidarea și eficientizarea legislației în materie de protecție a datelor, cum ar fi posibilitatea oferită entităților legale de a iniția măsuri în ceea ce privește violarea protecției datelor și obligația impusă controlorilor de date de a notifica încălcările securității.

12. În pofida unei abordări generale favorabile, AEPD regretă faptul că propunerea nu este atât de ambițioasă pe cât ar fi putut fi. Într-adevăr, din 2003, aplicarea dispozițiilor cuprinse în Directiva privind confidențialitatea în mediul electronic, precum și analiza aprofundată a subiectului au arătat că anumite dispoziții nu sunt încă suficient de clare, cauzând probleme de incertitudine juridică și de conformitate. Un exemplu de astfel de caz îl constituie cunoașterea măsurii în care furnizorii de servicii de comunicații electronice semipublice fac obiectul Directivei privind confidențialitatea în mediul electronic. Ar fi fost de așteptat ca Comisia să utilizeze revizuirea pachetului telecomunicații și, în special, a Directivei privind confidențialitatea în mediul electronic pentru a soluționa unele dintre problemele restante. În plus, propunerea oferă numai o soluție parțială în abordarea noilor aspecte precum instituirea unui sistem de notificare obligatorie privind încălcarea securității, deoarece nu include în domeniul de aplicare a organizațiilor supuse obligației de a notifica încălcările securității entitățile care prelucrează date foarte sensibile, cum ar fi băncile on-line sau furnizorii de servicii medicale on-line. AEPD regretă această abordare.

13. AEPD speră că, pe măsură ce propunerea avansează în procesul legislativ, organul legislativ va ține seama de comentariile și propunerile cuprinse în prezentul aviz pentru a soluționa aspectele pe care propunerea Comisiei nu le-a abordat.

([1]) Avizul Autorității Europene pentru Protecția Datelor 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).

II. ANALIZA PROPUNERII

II.1. Domeniul de aplicare a Directivei privind confidențialitatea în mediul electronic, în special serviciile implicate

14. Un aspect-cheie în cadrul Directivei privind confidențialitatea în mediul electronic în vigoare îl reprezintă domeniul de aplicare a acesteia. Propunerea include anumite elemente favorabile definirii și clarificări domeniului de aplicare a directivei, în special, serviciile vizate de directivă, care sunt discutate la punctul (i). Din păcate, modificările propuse nu soluționează toate problemele existente. Astfel cum s-a discutat la punctul (ii), din păcate, modificările nu urmăresc să extindă domeniul de aplicare a directivei pentru a include serviciile de comunicații electronice în rețele private.

15. Articolul 3 din Directiva privind confidențialitatea în mediul electronic descrie serviciile care fac obiectul directivei, cu alte cuvinte, serviciile cărora li se aplică obligația prevăzută în directivă: „*Prezenta directivă se aplică prelucrării de date personale legate de furnizarea de servicii de comunicații electronice prin intermediul rețelelor de comunicații electronice din cadrul Comunității*".

16. Prin urmare, serviciile care fac obiectul Directivei privind confidențialitatea în mediul electronic sunt cele oferite de furnizorii de servicii de comunicații electronice în rețele publice („FSCEP") Definiția unui FSCEP este prevăzută la articolul 2 litera (c) din directiva-cadru ([1]). Rețelele publice de comunicații sunt definite la articolul 2 litera (d) din directiva-cadru ([2]). Printre activitățile unui FSCEP se numără furnizarea accesului la internet, transmiterea de informații prin rețele electronice, conectarea la o rețea de telefonie fixă sau mobilă, etc.

(i) *Modificare propusă la articolul 3 din Directiva privind confidențialitatea în mediul electronic: Serviciile implicate, astfel încât să includă rețelele de comunicații publice care presupun colectare de date și mecanisme de identificare*

17. Propunerea modifică articolul 3 din Directiva privind confidențialitatea în mediul electronic, specificând că rețelele de comunicații electronice publice includ „*rețelele de comunicații publice care presupun colectare de date și mecanisme de identificare*". Considerentul 28 explică că dezvoltarea aplicațiilor care rezultă în colectarea de informații, inclusiv de date personale, utilizând frecvențele radio, precum RFID, trebuie să se supună Directivei privind confidențialitatea în mediul electronic atunci când sunt conectate la rețelele sau serviciile de comunicații publice sau atunci când le utilizează pe acestea.

18. AEPD consideră pozitivă această dispoziție deoarece clarifică faptul că un număr de aplicații RFID sunt incluse în domeniul de aplicare a Directivei privind confidențialitatea în mediul electronic, eliminând astfel o anumită incertitudine pe marginea acestui punct și eliminând definitiv înțelegerile sau interpretările greșite ale legislației.

19. Într-adevăr, în temeiul actualului articol 3 din Directiva privind confidențialitatea în mediul electronic, anumite aplicații RFID sunt deja reglementate de directiva în cauză. Există mai multe motive cumulative pentru această reglementare. În primul rând, deoarece aplicațiile RFID sunt incluse în definiția serviciilor de comunicații electronice. În al doilea rând, pentru că sunt furnizate printr-o rețea de comunicații electronice în măsura în care aplicațiile sunt acceptate de un sistem de transmisie care

([1]) Directiva 2002/21/CE a Parlamentului European și a Consiliului din 7 martie 2002 privind un cadru de reglementare comun pentru rețelele și serviciile de comunicații electronice (JO L 108, 24.4.2002, p. 33). Directiva-cadru definește conceptul de serviciu de comunicații electronice, și anume: (i) „Serviciu de comunicații electronice" înseamnă serviciul furnizat de obicei contra cost și care constă în transmiterea de semnale prin rețele de comunicații electronice și include serviciile de telecomunicații și serviciile de transmisie prin rețele. (ii) Serviciile care constau din furnizarea de conținuturi prin intermediul rețelelor și serviciilor de comunicații electronice sunt excluse din definiția serviciilor de comunicații electronice. (iii) Furnizarea de servicii înseamnă instalarea, operarea, supravegherea sau punerea la dispoziție a unei rețele. (iv) Serviciile de comunicații electronice nu includ serviciile societății informaționale, care sunt definite în Directiva privind comerțul electronic drept serviciu(i) prestat(e) în scopul obținerii unei remunerații, la distanță, prin mijloace electronice și la solicitarea individuală a beneficiarului serviciilor.

([2]) Rețea publică de comunicații înseamnă o rețea de comunicații electronice utilizată, în întregime sau în principal, pentru furnizarea de servicii de comunicații electronice destinate publicului.

transmite semnale fără fir. În ultimul rând, rețeaua poate fi publică, dar și privată. Dacă sunt publice, aplicațiile RFID vor fi considerate „servicii implicate" și vor intra astfel sub incidența domeniului de aplicare a Directivei privind confidențialitatea în mediul electronic. Cu toate acestea, modificarea propusă va elimina orice îndoială restantă și va oferi în consecință o certitudine juridică suplimentară.

20. Desigur, după cum s-a indicat în avizul anterior al AEPD privind RFID ([1]), această dispoziție nu înlătură eventuala necesitate de a aplica anumite instrumente juridice suplimentare în ceea ce privește RFID. Astfel de măsuri ar trebui adoptate însă într-un context diferit, și nu ca parte a propunerii în cauză.

(ii) *Necesitatea de a include serviciile de comunicații electronice în rețele private sau semiprivate*

21. Deși consideră binevenită clarificarea descrisă mai sus, AEPD regretă că propunerea nu a abordat aspectul distincției tot mai vagi dintre rețelele private și cele publice. AEPD regretă de asemenea faptul că definiția serviciilor reglementate de Directiva privind confidențialitatea în mediul electronic nu a fost lărgită pentru a include rețelele private. În forma actuală, articolul 3 alineatul (1) din Directiva privind confidențialitatea în mediul electronic se aplică doar *serviciilor de comunicații electronice în rețelele publice*.

22. AEPD constată tendința serviciilor de a deveni tot mai pregnant un amalgam de servicii private și publice. Un astfel de exemplu sunt universitățile care permit miilor de studenți să folosească internetul și emailul. Abilitatea acestor rețele semipublice (sau semiprivate) de a afecta viața privată a persoanelor este evidentă, impunând astfel supunerea acestui tip de servicii aceluiași tip de norme ca cele care se aplică rețelelor exclusiv publice. În plus, rețelele private de tipul rețelelor de angajatori care oferă angajaților acces la internet, de proprietari de hoteluri sau apartamentele care pun la dispoziția oaspeților telefon și email, precum și cafenelele internet, au un impact asupra protecției datelor și a confidențialității utilizatorilor acestora, ceea ce sugerează că și aceștia ar trebui să intre sub incidența domeniului de aplicare a Directivei privind confidențialitatea în mediul electronic.

23. De fapt, jurisprudența anumitor state membre a supus deja serviciile de comunicații electronice furnizate în rețelele private acelorași obligații ca cele furnizate în rețelele publice ([2]). Mai mult, conform legislației germane, autoritățile de protecție a datelor au constatat că permiterea utilizării emailului privat în cadrul unei societăți poate duce la considerarea respectivei societăți drept operator de servicii de telecomunicații publice și, în consecință, la încadrarea acesteia sub incidența dispozițiilor Directivei privind confidențialitatea în mediul electronic.

24. Pe scurt, importanța tot mai crescută a rețelelor mixte (private/publice) și private în viața zilnică, însoțită de creșterea corespunzătoare a riscului la care sunt supuse datele personale și confidențialitatea, justifică necesitatea de a aplica acestor servicii același set de norme care se aplică serviciilor de comunicații electronice publice. AEPD consideră în acest scop că directiva ar trebui modificată, astfel încât domeniul de aplicare a acesteia să fie extins, pentru a include un astfel de tip de servicii private; această opinie este împărtășită și de Grupul de lucru 29 ([3]).

II.2. **Notificarea încălcărilor securității: Modificare la articolul 4**

25. Articolul 4 din Directiva privind confidențialitatea în mediul electronic este modificat prin includerea a două noi alineate [(3) și (4)], care stabilesc obligația de a notifica încălcările securității. Într-adevăr, potrivit articolului 4 alineatul (3), FSCEP sunt obligați, pe de o parte, să notifice autorităților naționale de reglementare, fără întârzieri nejustificate, orice încălcare a securității având ca rezultat distrugerea accidentală sau ilegală, pierderea, alterarea, divulgarea neautorizată sau accesul neautorizat la datele personale transmise, stocate sau prelucrate în alt mod în legătură cu furnizarea de servicii de comunicații electronice (la modul general „compromiterea datelor"); pe de altă parte, FSCEP sunt de asemenea obligați să își înștiințeze clienții.

([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.

([2]) De exemplu, hotărârea Curții de Apel de la Paris în cazul *BNP Paribas* împotriva *World Press Online*, emisă la 4 februarie 2005, a constatat că nu există nicio deosebire între furnizorii de servicii internet care au oferit accesul la internet pe o bază comercială și furnizorii care au oferit acces la internet personalului lor.

([3]) Avizul 8/2006 privind revizuirea cadrului de reglementare pentru comunicațiile și serviciile electronice, cu accentul pe Directiva privind confidențialitatea în mediul electronic adoptată la 26 septembrie 2006.

Beneficiile acestei obligații

26. AEPD salută aceste dispoziții [articolul 4 alineatele (3) și (4)], care introduc un aviz obligatoriu privind notificarea încălcărilor securității. Notificarea încălcărilor securității are efecte pozitive din perspectiva protecției datelor personale și a confidențialității, care au fost deja testate în Statele Unite, unde există de câțiva ani deja, la nivel de stat, o legislație privind notificarea încălcărilor.

27. În primul rând, legislația privind notificarea încălcărilor sporește responsabilitatea FSCEP în privința informațiilor care au fost compromise. În temeiul cadrului strategic privind protecția datelor sau confidențialitatea, responsabilitatea înseamnă că fiecare organizație răspunde de informațiile de care dispune și pe care le controlează. Obligația notificării este deosebit de importantă pentru a declara din nou, pe de o parte, că datele care au fost compromise erau sub controlul FSCEP și, pe de altă parte, că adoptarea măsurilor necesare referitoare la aceste date face parte din responsabilitatea acestei organizații.

28. În al doilea rând, existența unei notificări a încălcării securității s-a dovedit a fi un factor care orientează investițiile în materie de securitate către organizațiile care prelucrează date personale. Într-adevăr, simpla obligație de a notifica în mod public încălcările securității determină organizațiile să pună în aplicare standarde de securitate mai stricte, care protejează informațiile personale și care previn încălcările. Mai mult decât atât, notificarea încălcărilor securității va contribui la identificarea și realizarea unor analize statistice fiabile în ceea ce privește cele mai eficiente soluții și mecanisme de securitate. Pentru o lungă perioadă de timp, au existat insuficiente date solide despre defecțiunile apărute în securitatea informațiilor și despre cele mai adecvate tehnologii de protejare a informațiilor. Este posibil ca această problemă să se rezolve odată cu obligațiile de notificare a încălcării securității, așa cum a fost cazul legislației SUA de raportare a încălcării securității, deoarece notificarea va furniza informații asupra tehnologiilor care înlesnesc încălcările ([1]).

29. În sfârșit, notificarea încălcărilor securității îi face pe indivizi mai conștienți de riscul cu care se confruntă atunci când datele personale le sunt compromise și îi ajută să ia măsurile necesare pentru a reduce aceste riscuri. De exemplu, dacă au fost compromise date bancare, persoana care este informată în acest sens poate decide să își schimbe detaliile de accesare ale contului bancar pentru a evita ca cineva să preia aceste informații și să le utilizeze în scopuri ilegale (act denumit în mod normal „furt de identitate"). În concluzie, această obligație reduce posibilitatea ca indivizii să devină victime ale furtului de identitate și ajută victimă să întreprindă acțiunile necesare pentru soluționarea problemelor.

Dezavantajul modificării propuse

30. Deși este mulțumită de sistemul de notificare a încălcării securității prevăzut la articolul 4 alineatele (3) și (4), AEPD ar fi preferat ca acestea să fie aplicate la o scară mai largă, astfel încât să includă furnizorii de servicii ale societății informaționale. Aceasta ar presupune ca băncile on-line, afacerile on-line, furnizorii de servicii medicale on-line etc. să intre de asemenea sub incidența legislației în cauză ([2]).

31. Motivul care justifică impunerea unei notificări a încălcării securității în cazul furnizorilor de servicii de comunicații electronice publice, sau FSCEP, există și în ceea ce privește alte organizații care prelucrează mari volume de date personale, a căror divulgare ar putea fi deosebit de dăunătoare persoanelor vizate. Sunt incluse aici băncile on-line, brokerii de date și alți furnizori on-line, cum sunt cei care prelucrează date sensibile (printre care se numără datele medicale, opiniile politice etc.). Compromiterea informațiilor deținute de băncile on-line și de afacerile on-line, care pot include nu doar numere de conturile bancare, dar și detalii ale cărții de credit, poate conduce la un furt de identitate, caz în care este esențial să se atragă atenția persoanelor în cauză, pentru ca acestea să ia măsurile necesare. În cazul din urmă (servicii medicale on-line), atunci când sunt compromise informații sensibile, este posibil ca persoanele să sufere, dacă nu pagube financiare, cu siguranță pagube de natură non-economică.

([1]) A se vedea raportul „*Security Economics and the Internal Market*" (Economia securității și piața internă), solicitat de ENISA prof. Ross Anderson, Rainer Böhme, Richard Clayton și Tyler Moore. Raportul poate fi consultat la: http://www.enisa.europa.eu/doc/pdf/report_sec_econ_&_int_mark_20080131.pdf

([2]) Furnizorii de servicii ale societății informaționale sunt definiți de Directiva privind comerțul electronic drept serviciu(i) prestat(e) în scopul obținerii unei remunerații, la distanță, prin mijloace electronice și la solicitarea individuală a beneficiarului serviciilor.

32. Pe lângă aceasta, odată cu extinderea domeniului de aplicare a obligației, beneficiile descrise mai sus, care se așteaptă să decurgă din impunerea acestei obligații, nu vor fi limitate la un sector de activitate, cel al furnizorilor de servicii de comunicații electronice disponibile publicului, ci vor fi extinse serviciilor societății informaționale în general. Într-adevăr, impunerea obligațiilor de notificare a încălcării securității asupra serviciilor societății informaționale de tipul băncilor on-line nu doar va spori responsabilitatea acestora, ci va și motiva astfel de actori să își consolideze măsurile de securitate și să evite pe viitor potențialele încălcări ale securității.

33. Există și alte precedente în care Directiva privind confidențialitatea în mediul electronic se aplică deja altor entități decât FSCEP, cum sunt articolul 5 privind confidențialitatea comunicațiilor și articolul 13 privind spam-urile. Se confirmă astfel că, în trecut, dând dovadă de multă prudență, legiuitorul a luat decizia de a lărgi domeniul de aplicare a anumitor dispoziții din Directiva privind confidențialitatea în mediul electronic deoarece a considerat această acțiune adecvată și necesară. AEPD speră că, în prezent, legiuitorul nu va ezita să adopte o abordare similară, prudentă și flexibilă, și nici să extindă domeniul de aplicare a articolului 4, astfel încât să includă furnizorii de servicii ale societății informaționale. În acest scop, ar fi suficient să se introducă în articolul 4 alineatul (3) o trimitere la furnizorii de servicii ale societății informaționale, după cum urmează: „În cazul unei încălcări a securității având ca rezultat distrugerea accidentală sau … furnizorul de servicii de comunicații accesibile publicului și furnizorul de servicii ale societății informaționale notifică … abonatul în cauză și autoritățile naționale de reglementare cu privire la o astfel de încălcare”.

34. AEPD consideră că această obligație și aplicarea ei atât în cazul FSCEP, cât și al furnizorilor de servicii ale societății informaționale sunt un prim pas într-o evoluție care ar putea în cele din urmă să fie aplicată tuturor controlorilor de date în general.

Cadrul juridic specific pentru abordarea încălcărilor securității prin intermediul comitologiei

35. Propunerea nu abordează o serie de aspecte care privesc obligația de notificare a încălcărilor securității. Exemple de astfel de aspecte care trebuie abordate sunt împrejurările înștiințării, formatul și procedurile aplicabile. În schimb, articolul 4 alineatul (4) al propunerii prevede că respectivele decizii urmează să fie adoptate de către un comitet de tipul celor prevăzute în procedurile în materie de comitologie ([1]), și anume Comitetul pentru comunicații instituit prin articolul 22 din directiva-cadru, în temeiul Deciziei Consiliului din 28 iunie 1999. În particular, astfel de măsuri ar fi adoptate în conformitate cu articolul 5 din Decizia Consiliului din 28 iunie 1999 care stabilește regulile privind procedura de reglementare, referitor la „măsuri cu domeniu general de aplicare concepute să pună în aplicare prevederile esențiale ale actelor de bază”.

36. AEPD nu se opune posibilității ca toate aceste aspecte să fie reglementate de legislația de punere în aplicare. Este foarte probabil ca adoptarea legislației prin intermediul comitologiei să scurteze procedura legislativă. De asemenea, comitologia va contribui la asigurarea armonizării, care reprezintă un obiectiv ce trebuie luat în considerare.

37. Luând în considerare numărul mare de aspecte care vor trebui abordate prin intermediul măsurilor de punere în aplicare, precum și relevanța acestora, după cum se evidențiază mai jos, este adecvat ca acestea să fie prevăzute într-un singur act legislativ, în locul unei abordări fragmentare, prin care o parte dintre aspecte să fie prevăzute de Directiva privind confidențialitatea în mediul electronic, în timp ce altele să fie prevăzute de legislația de punere în aplicare. Astfel, trebuie salutată abordarea Comisiei de a lăsa deciziile respective în sarcina legislației de punere în aplicare, care urmează să fie adoptată după consultarea AEPD și, în principiu, și a altor actori implicați (a se vedea punctul de mai jos).

Aspecte care vor trebui abordate prin intermediul măsurilor de punere în aplicare

38. Relevanța măsurilor de punere în aplicare este evidențiată dacă se prevede în mod destul de detaliat care sunt aspectele care trebuie abordate prin măsurile de punere în aplicare. Într-adevăr, măsurile de punere în aplicare pot determina standardele în conformitate cu care trebui făcute înștiințările. Acestea pot să prevadă de exemplu ce reprezintă o încălcare a securității, condițiile în conformitate cu care persoanele fizice și autoritățile sunt notificate, termenul de înștiințare și notificare.

([1]) Proceduri legislative din cadrul CE care implică comitete alcătuite din reprezentanți ai guvernelor statelor membre, la nivel de funcționari publici.

39. AEPD consideră că Directiva privind confidențialitatea în mediul informatic și în special articolul 4 nu ar trebui să prevadă nicio excepție de la obligația de notificare. În acest sens, AEPD este satisfăcută de abordarea Comisiei cuprinsă în articolul 4 care stabilește o obligație de notificare și nu prevede nicio excepție de la aceasta, dar permite ca acest aspect, precum și altele, să fie abordate de legislația de punere în aplicare. Cu toate că AEPD este conștientă de argumentele care ar putea justifica instituirea unor excepții de la obligația respectivă, AEPD se pronunță în favoarea abordării aspectului în cauză, precum și a altora, prin legislația de punere în aplicare, după o dezbatere detaliată și globală a tuturor aspectelor de interes. După cum s-a arătat mai sus, natura complexă a obligației de furnizare a notificării cu privire la încălcările de securitate, inclusiv dezbaterea referitoare la gradul de adecvare al excepțiilor sau al limitărilor, impune abordarea acesteia în mod unitar, adică în cadrul unui singur act legislativ care să se refere numai acest aspect.

Consultarea Autorității Europene pentru Protecția Datelor și necesitatea extinderii consultării

40. Luând în considerare proporția în care măsurile de punere în aplicare vor afecta protecția datelor personale ale persoanelor fizice, este important ca anterior adoptării acestor măsuri, Comisia să organizeze o consultare adecvată. Din acest motiv, AEPD salută articolul 4 alineatul (4) din propunere care prevede în mod explicit că anterior adoptării măsurilor de punere în aplicare, Comisia va consulta Autoritatea Europeană pentru Protecția Datelor. Astfel de măsuri nu doar vor viza, ci vor avea un impact important asupra protecției datelor personale și a vieții private a persoanelor fizice. De aceea este important să se solicite avizul AEPD, astfel cum se prevede la articolul 41 din Regulamentul (CE) nr 45/2001.

41. În plus față de consultarea AEPD, poate fi adecvată includerea unei dispoziții care să prevadă că măsurile de punere în aplicare vor face obiectul unei consultări publice, în vederea obținerii unor opinii și pentru a încuraja schimbul de experiență și de cele mai bune practici în domeniu. Aceasta va garanta existența unei modalități adecvate prin care nu numai industria, ci și alți actori interesați, inclusiv alte autorități de protecție a datelor și Grupul de lucru „articolul 29" să își exprime opiniile. Necesitatea unei consultări publice este consolidată dacă se ține cont de faptul că procedura de adoptare a legislației este comitologia, care presupune o intervenție limitată a Parlamentului European.

42. AEPD ia act de faptul că articolul 4 alineatul (4) din propunere prevede că Comisia va consulta de asemenea Autoritatea europeană de reglementare a pieței de comunicații electronice, anterior adoptării normelor de punere în aplicare. În acest sens, AEPD apreciază principiul consultării Autorității europene de reglementare a pieței de comunicații electronice ca depozitar al experienței ENISA și a cunoștințelor privind aspectele legate de rețea și de securitatea informațiilor. Până la crearea Autorității europene de reglementare a pieței de comunicații electronice, includerea în modificarea propusă [articolul 4 alineatul (4)] a consultării ENISA poate reprezenta o soluție interimară adecvată.

II.3. **Dispoziții privind „cookies", „spyware" și alte instrumente similare Modificare la articolul 5 alineatul (3)**

43. Articolul 5 alineatul (3) din Directiva privind confidențialitatea în mediul electronic abordează aspectele referitoare la tehnologiile care permit accesul la informație și stocarea de informații în echipamentul terminal al utilizatorului, prin intermediul rețelelor de comunicații electronice. Utilizarea de cookies ([1]) reprezintă un exemplu de aplicare a articolului 5 alineatul (3). Alte exemple includ utilizarea unor tehnologii precum spyware (programe ascunse de spionaj) și programele disimulate (trojan horses — programe ascunse în mesaje sau în soft-uri aparent curate). Scopul unor astfel de tehnologii și obiectivele variază foarte mult, deoarece dacă unele nu au niciun fel de efecte negative și pot fi chiar utile pentru utilizator, altele sunt în mod clar negative și dăunătoare.

([1]) Cookies sunt plasate de FSSI (furnizori de serivcii ale societății informaționale) în echipamentele terminale ale utilizatorului, în vederea a diferite scopuri, inclusiv recunoașterea unui vizitator atunci când acesta revizitează un site web. În practică, în situația în care o cookie este trimisă unui utilizator internet de către un site web, computerului utilizatorului i se atribuie un număr unic (de exemplu, computerul care a primit o cookie de la site-ul web A devine „computer deținător al cookie 111"). Site-un web păstrează acest număr ca referință. Dacă utilizatorul(ii) computerului care a primit cookie 111 nu elimină dosarul cookie, data viitoare când acesta/aceștia vizitează același site web, respectivul site va putea identifica computerul ca fiind deținătorul cookie 111. Site-ul web deduce în mod logic că respectivul computer a vizitat anterior pagina. Mecanismul care permite unui site web să recunoască un computer care vizitează de mai multe ori este unul simplu. În situația în care, computerul respectiv deține cookies, ca de exemplu cookie 111, și vizitează site-ul care la o vizită anterioară a generat cookie în cauză, va căuta pe hard disk-ul utilizatorului numărul dosarului cookie. Dacă browser-ul utilizatorului găsește un dosar cookie care are același număr de referință ca și numărul păstrat de site-ul web, va informa respectivul site că computer-ul deține o cookie 111.

44. Articolul 5 alineatul (3) din Directiva privind confidențialitatea în mediul electronic stabilește condițiile privind obținerea accesului la sau stocare de informații pe echipamentul de terminal al utilizatorilor care întrebuințează, printre altele, tehnologiile sus-menționate. În special, în temeiul articolului 5 alineatul (3): (i) utilizatorii de internet trebuie să primească informații clare și complete, între altele cu privire la obiectivele prelucrării, în conformitate cu Directiva 95/46/CE; și (ii) utilizatorilor internet trebuie să le se permită să refuze astfel de prelucrări, de exemplu să se retragă din procedura de prelucrare a informațiile extrase din echipamentul lor terminal.

Avantajele modificării propuse

45. Actualul articol 5 alineatul (3) din Directiva privind confidențialitatea în mediul informatic limitează domeniul de aplicare al acesteia la situațiile în care accesul la informație și stocarea de informații în echipamentul terminal al utilizatorului se realizează prin intermediul *rețelelor de comunicații electronice*. Această include situația sus-menționată referitoare la utilizarea de cookies, precum și a altor tehnologii precum spyware, furnizate prin rețele de comunicații electronice. Cu toate acestea, nu este deloc clar dacă articolul 5 alineatul (3) se aplică în situații în care tehnologii similare (cookies/spyware și altele de acest tip) sunt distribuite prin intermediul soft-urilor furnizate pe mediile externe de stocare a datelor și descărcate în echipamentul terminal al utilizatorului. Având în vedere faptul că amenințarea față de viața privată există în mod independent de canalul de comunicare, faptul că articolul 5 alineatul (3) se limitează la un singur canal de comunicare nu reprezintă un aspect pozitiv.

46. AEPD își exprimă satisfacția cu privire la modificările la articolul 5 alineatul (3) care, prin eliminarea trimiterii la „rețele de comunicații electronice" extinde de fapt domeniul de aplicare a articolului 5 alineatul (3). Într-adevăr, versiunea modificată a articolului 5 alineatul (3) cuprinde ambele situații în care accesul la informație și stocarea de informații în echipamentul terminal al utilizatorului se realizează atât prin intermediul unor rețele de comunicații electronice cât și prin alte medii externe de stocare a datelor, precum CD-urile, CD-ROM-urile, cheile USB etc.

Stocarea tehnică în scopul facilitării transmisiei

47. Ultima teză a articolului 5 alineatul (3) din Directiva privind confidențialitatea în mediul electronic rămâne neschimbată în versiunea modificată a acestuia. În temeiul ultimei teze, cerințele primei teze a articolului 5 alineatul (3) „*… nu interzic stocarea sau accesul tehnic cu unicul scop de a efectua sau de a facilita transmisia comunicației printr-o rețea de comunicații electronice sau în cazul în care acest lucru este strict necesar în vederea furnizării unui serviciu al societății informaționale …*". Astfel, regulile obligatorii prevăzute la prima teză a articolului 5 alineatul (3) (necesitatea de a furniza informații și oferirea posibilității de refuz) nu se vor aplica în situația în care accesul la echipamentul terminal al utilizatorului sau stocarea informațiilor au drept scop unic *facilitarea* unei transmiteri sau când sunt absolut necesare pentru furnizarea unor servicii ale societății informaționale solicitate de utilizator.

48. Directiva nu prevede situația în care accesul sau stocarea de informații au drept scop unic facilitarea unei transmiteri sau furnizarea de informații. O situație care ar intra în mod clar sub incidența respectivei excepții o reprezintă stabilirea unei conexiuni internet. Acest lucru se întâmplă deoarece stabilirea unei conexiuni internet este necesară pentru obținerea unei adrese IP ([1]). Computerului utilizatorului final i se va solicita să divulge furnizorului de acces la internet anumite informații despre sine, în schimbul cărora furnizorul de acces la internet îi va oferi o adresă IP. În această situație, informațiile stocate în echipamentul terminal al utilizatorului final vor fi transferate către furnizorul e acces la internet, pentru a-i oferi utilizatorului acces la internet. Astfel, furnizorul de acces la internet este scutit atât de obligația de a anunța respectiva colectare de informații cât și de a oferi dreptul de refuz, în măsura în care informațiile respective sunt necesare pentru furnizarea serviciului.

49. Odată conectat la internet, dacă utilizatorul dorește să acceseze o anumită pagină web, acesta trebuie să trimită o cerere către server-ul pe care se găsește respectiva pagină. Serverul în cauză va răspunde dacă știe unde să trimită informația, adică dacă cunoaște adresa IP a utilizatorului. Din cauza modalității de stocare a respectivei adrese, site-ul web pe care utilizatorul dorește să îl viziteze trebui să acceseze din nou informații de pe echipamentul terminal al utilizatorului de internet. În mod clar și această tranzacție intră sub incidența excepției. Într-adevăr, pare adecvat ca aceste situații să nu intre sub incidența cerințelor prevăzute la articolul 5 alineatul (3).

([1]) O adresă IP (adresă de protocol internet) este o adresă unică pe care anumite echipamente electronice o utilizează pentru a se identifica și a comunica între ele, intr-o rețea de computere care folosesc protocolul internet standard (IP) — în termeni mai simpli, o adresă de computer. Orice echipament de rețea participant — inclusiv dispozitive care interconectează mai multe rețele locale (router), dispozitive de comutare (switch), computere, servere de infrastructură (de exemplu NTP, DNS, DHCP, SNMP, etc.), imprimante, fax-uri pentru internet și o serie de telefoane — pot avea propria lor adresă în câmpul de aplicare al unei rețele specifice. O serie de adrese IP sunt concepute pentru a fi unice în câmpul de aplicare al internetului global, în timp ce altele sunt concepute pentru a fi unice în câmpul de aplicare al unei întreprinderi.

50. AEPD consideră că este adecvat ca situații precum cele descrise mai sus să fie scutite de necesitatea de informare și de oferire a posibilității de refuz, dacă stocarea tehnică sau accesul la echipamentul terminal al unui utilizator sunt *necesare* în scopul unic al transmiterii unei comunicări prin intermediul unei rețele de comunicații electronice. Același principiu se aplică și în situația în care stocarea tehnică sau accesul sunt strict necesare pentru furnizarea unui serviciu al societății informaționale. Cu toate acestea, AEPD nu consideră că este necesară excluderea de la obligația de furnizare a informațiilor și de oferire a dreptului de refuz în acele situații în care stocarea tehnică sau accesul au drept scop simpla *facilitare* a transmiterii sau a comunicării. De exemplu, în temeiul ultimei teze a articolului respectiv persoana vizată nu poate beneficia de informare și de dreptul de a se opune la prelucrarea datelor sale dacă o cookie îi colectează preferințele lingvistice sau locația (de exemplu Belgia, China), deoarece acest tip de cookie ar putea fi prezentată ca având drept scop facilitarea transmiterii unei comunicări. AEPD este conștientă de faptul că la nivelul de soft, în practică se oferă persoanelor vizate posibilitatea de a refuza sau de a modula stocarea de cookies. Totuși aceasta nu este susținută în mod destul de clar de nicio dispoziție juridică care să confere în mod formal persoanei vizate dreptul să își protejeze drepturile în contextul descris mai sus.

51. Pentru a evita acest rezultat, AEPD sugerează efectuarea unei modificări minore în ultima parte a articolului 5 alineatul (3), care constă în eliminarea cuvântului „a facilita" din propoziție: „*… nu împiedică stocarea sau accesul tehnic cu unicul scop de a efectua sau de a facilita transmisia comunicației printr-o rețea de comunicații electronice sau, în cazul în care acest lucru este strict necesar, în vederea furnizării unui serviciu al societății informaționale …*".

II.4. **Acțiuni judiciare inițiate de FSCEP și persoane juridice: Adăugarea alineatului (6) la articolul 13**

52. Articolul 13 alineatul (6) care a fost propus oferă reparații civile pentru orice persoană fizică sau juridică având interese legitime, în special pentru furnizorii de servicii de comunicații electronice care au interese legate de afaceri pentru a lupta împotriva celor care încalcă dispozițiile articolului 13 din Directiva privind confidențialitatea în mediul electronic. Acest articol reglementează trimiterea de comunicări comerciale nesolicitate.

53. Modificarea propusă va permite, de exemplu, furnizorilor de acces la internet să se ocupe de „spammer"-ii care folosesc abuziv rețelele, să intenteze acțiuni în instanță împotriva entităților care se ocupă cu contrafacerea adreselor expeditorului sau hackingul serverelor pentru utilizarea lor ca puncte de transfer al mesajelor spam.

54. Nu reieșea clar din Directiva privind confidențialitatea în mediul electronic dacă FSCEP aveau dreptul de a acționa împotriva „spammer"-ilor și, de câteva ori, FSCEP au introdus acțiuni în fața instanțelor pentru încălcarea dispozițiilor articolului 13, astfel cum a fost pus în aplicare în legislația statului membru ([1]). Recunoscând acțiunea în justiție pentru furnizorii de servicii de comunicații electronice pentru a își proteja interesele de afaceri, propunerea confirmă faptul că Directiva privind confidențialitatea în mediul electronic intenționează să protejeze nu numai abonații (care sunt) persoane fizice, dar și furnizorii de servicii de comunicații electronice.

55. AEPD este mulțumită că propunerea introduce posibilitatea ca furnizorii de servicii de comunicații electronice care au un interes legat de afaceri să acționeze în instanță „spammer"-ii. În afara unor situații excepționale, persoanele fizice abonate nu au nici banii, nici stimulentele pentru a iniția aceste tip de acțiune în instanță. În schimb, furnizorii de acces la internet și alți FSCEP au puterea financiară și capacitatea tehnologică pentru a investiga campaniile de trimitere de spam, pentru a identifica făptașii;pare firesc ca aceștia să aibă dreptul de a acționa „spammer"-ii în judecată.

56. AEPD apreciază în mod special modificarea propusă în măsura în care ar permite, de asemenea, asociațiilor de consumatori și sindicatelor care reprezintă interesele consumatorilor afectați de spam să acționeze în instanță în numele acestora din urmă. După cum s-a subliniat mai sus, daunele cauzate unei persoane vizate care a fost afectată de spam, luate în mod individual, nu sunt în general suficiente în sine pentru ca persoana respectivă să intenteze o acțiune judiciară în instanță. De fapt, AEPD a propus deja această măsură în ceea ce privește încălcarea confidențialității și a protecției datelor la

([1]) Unul dintre aceste cazuri este corporația Microsoft versus/împotriva Paul McDonald t/a Bizards UK [2006 All Er (D) 153].

modul general în Avizul cu privire la continuarea programului de lucru pentru o mai bună punere în aplicare a Directivei privind protecția datelor ([1]). În opinia AEPD, propunerea ar fi putut fi și mai detaliată, propunând acțiuni colective, care să permită unor grupuri de cetățeni să introducă acțiuni în justiție comune în materie de protecție a datelor personale. În cazul spamului, atunci când foarte multe persoane primesc acest tip de corespondență nesolicitată, există posibilitatea ca grupuri de persoane să se unească și să introducă acțiuni comune împotriva „spammer"-ilor.

57. AEPD regretă în mod special faptul că propunerea limitează posibilitatea persoanelor juridice de a intenta o acțiune în justiție în situații în care există o încălcare a articolului 13 din directivă, i.e. situații în care are loc o încălcare a dispoziției privind comunicările nesolicitate prin email. Într-adevăr, în conformitate cu modificarea propusă, persoanele juridice nu ar avea capacitatea de a intenta o acțiune în justiție atunci când este vorba de încălcări ale altor dispoziții ale Directivei privind confidențialitatea în mediul electronic. De exemplu, dispoziția actuală nu permite unei persoane juridice, precum o asociație de consumatori, să acționeze în judecată un furnizor de servicii de acces la internet care a dezvăluit datele personale a milioane de clienți. Aplicarea Directivei privind confidențialitatea în mediul electronic în întregul său, și nu numai a unui articol anume, ar fi substanțial îmbunătățită dacă dispoziția articolului 13 alineatul (6) ar fi generalizată pentru a permite persoanelor juridice să intenteze o acțiune în justiție atunci când este vorba de încălcări ale oricăror dispoziții ale Directivei privind confidențialitatea în mediul electronic.

58. Pentru a remedia această problemă, AEPD sugerează transformarea articolului 13 alineatul (6) într-un articol separat (articolul 14). În plus, formularea de la articolul 13 alineatul (6) ar trebui ușor modificată, după cum urmează: Acolo unde apare „în conformitate cu prezentul articol", ar trebui să apară „în conformitate cu prezenta directivă".

II.5. **Consolidarea dispozițiilor de punere în aplicare: Adăugarea articolului 15a**

59. Directiva privind confidențialitatea în mediul electronic nu conține dispoziții exprese de punere în aplicare. În schimb, se referă la secțiunea de punere în aplicare a Directivei privind protecția datelor ([2]). AEPD salută noul articolul 15a din propunere care reglementează în mod explicit chestiunile referitoare la punerea în aplicare în conformitate cu prezenta directivă.

60. În primul rând, AEPD ia notă de faptul că o politică eficientă de punere în aplicare în acest domeniu presupune că, după cum se solicită în conformitate cu articolul 15a alineatul (3) propus, autoritățile naționale au competențe de investigare pentru a aduna informațiile necesare. Adesea, probele încălcării dispozițiilor Directivei privind confidențialitatea în mediul electronic sunt de natură electronică și pot fi stocate pe diverse calculatoare sau instrumente și rețele. În acest context, este important ca autoritățile de aplicare a legii să aibă posibilitatea de a obține mandate de percheziție care să le permită intrarea, percheziția și confiscarea.

61. În al doilea rând, AEPD salută în mod special modificarea propusă, mai precis articolul 15a alineatul (2), conform căruia autoritățile naționale de reglementare trebuie să aibă competența de a solicita acțiuni în încetare, mai exact încetarea încălcărilor, și trebuie să aibă competențele și resursele de investigare necesare. Autoritățile naționale de reglementare, inclusiv autoritățile naționale de protecție a datelor, ar trebui să aibă competența de a impune acțiuni în încetare, care să îi împiedice pe făptași să continue o activitate prin care încalcă Directiva privind confidențialitatea în mediul electronic. Acțiunile în încetare sau competența de a ordona o încetare a unei încălcări este un instrument folositor în cazul unui comportament constant care violează drepturile persoanelor. Acțiunile în încetare vor fi foarte folositoare pentru a opri încălcările dispozițiilor Directivei privind confidențialitatea în mediul electronic, precum violarea articolului 13 privind comunicările comerciale nesolicitate care, prin chiar natura sa, reprezintă un exemplu de comportament constant.

62. În al treilea rând, propunerea permite Comisiei să ia măsuri tehnice de punere în aplicare pentru a asigura o cooperare transfrontalieră eficientă în aplicarea legilor naționale [modificarea propusă sub forma articolului 15a alineatul (4)]. Experiența cooperării de până acum include acordul stabilit la inițiativa Comisiei de instituire a unei proceduri comune pentru tratarea plângerilor transfrontaliere referitoare la spam.

([1]) Avizul Autorității Europene pentru Protecția Datelor 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).

([2]) 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.

63. AEPD consideră că, dacă legislația sprijină autoritățile de reglementare în asistarea omologului acestora din alte țări, va asista, fără îndoială, punerea în aplicare transfrontalieră. În consecință, este potrivit ca propunerea să permită Comisiei să creeze condițiile pentru a asigura cooperarea transfrontalieră, inclusiv procedurile de utilizare în comun a informațiilor.

III. **CONCLUZII ȘI RECOMANDĂRI**

64. AEPD salută pe deplin propunerea. Modificările propuse consolidează protecția confidențialității și a datelor personale în sectorul comunicațiilor electronice și aceasta are loc în lipsa constrângerilor, fără a crea obstacole nejustificate și care nu sunt necesare pentru organizații. Mai precis, AEPD consideră că, în cea mai mare parte, modificările propuse nu ar trebui modificate în măsura în care îndeplinesc în mod corespunzător obiectivul urmărit. Punctul 69 de mai jos enumeră modificările pe care AEPD le dorește neschimbate.

65. Fără a aduce atingere aprecierii globale pozitive a propunerii, AEPD consideră că unele dintre modificări ar trebui îmbunătățite pentru a asigura faptul că acestea oferă în mod eficient o protecție adecvată a datelor personale și a vieții private a persoanelor. Aceasta este în special adevărat în ceea ce privește dispozițiile referitoare la notificarea încălcării securității și cele care reglementează acțiunile judiciare intentate de furnizorii de servicii de comunicații electronice pentru violarea dispozițiilor referitoare la spam. În plus, AEPD regretă faptul că propunerea nu reușește să abordeze anumite chestiuni, care nu au fost reglementate în mod adecvat în actuala Directivă privind confidențialitatea în mediul electronic, pierzându-se posibilitatea ca acest exercițiu de revizuire să soluționeze problemele restante.

66. Pentru a soluționa ambele probleme, adică chestiunile care nu au fost abordate în mod corespunzător în propunere și chestiunile care nu au fost abordate deloc, acest aviz a înaintat câteva proiecte de propuneri. Punctele 67 și 68 rezumă problemele și propun o anumită terminologie. AEPD solicită legiuitorului să țină seama de aceste propuneri, pe măsură ce propunerea avansează în procesul legislativ.

67. Modificările din propunere pe care AEPD le-ar prefera în mod clar modificate includ:

(i) **Notificarea încălcării securității**: așa cum este formulată, modificarea propusă care adaugă *articolul 4 alineatul (4)* se plică furnizorilor de servicii publice de comunicații electronice în rețele publice (furnizorii de servicii de internet — FSI, operatorii de rețea) care sunt obligați să notifice autoritățile naționale de reglementare și clienții în legătură cu încălcările securității. AEPD sprijină pe deplin această obligație. Totuși, AEPD consideră că obligația ar trebui să îi vizeze și pe furnizorii de servicii ale societății informaționale care prelucrează adesea informații personale sensibile. Astfel, băncile și asiguratorii on-line, furnizorii de servicii medicale on-line și orice alte afaceri on-line vor trebui să respecte această obligație.

În acest scop, AEPD sugerează introducerea, în articolul 4 alineatul (3), a unei trimiteri la furnizorii de servicii ale societății informaționale după cum urmează: „*În cazul unei încălcări a securității … furnizorul de servicii de comunicații accesibile publicului și furnizorul de servicii ale societății informaționale informează … abonatul în cauză și autoritatea națională de reglementare cu privire la o astfel de încălcare*".

(ii) **Acțiuni judiciare inițiate de furnizorii de servicii publice de comunicații electronice în rețele publice**: așa cum este formulată, modificarea propusă care adaugă *articolul 13 alineatul (6)* oferă reparații civile pentru orice persoană fizică sau juridică, în special pentru furnizorii de servicii de comunicații electronice pentru a combate încălcările dispozițiilor articolului 13 din Directiva privind confidențialitatea în mediul electronic, care reglementează problema spamului. AEPD este mulțumită de această/respectiva dispoziție. Totuși, AEPD nu vede sensul limitării acestei noi competențe la încălcarea prevăzută la articolul 13. AEPD sugerează prevederea posibilității persoanelor juridice de a intenta o acțiune în justiție în cazul încălcării oricărei dispoziții a Directivei privind confidențialitatea în mediul electronic.

Pentru a realiza acest lucru, AEPD sugerează transformarea articolului 13 alineatul (6) într-un articol separat (articolul 14). În plus, formularea de la articolul 13 alineatul (6) ar trebui ușor modificată, după cum urmează: Acolo unde apare „*în conformitate cu prezentul articol*", ar trebui să apară „în conformitate cu prezenta directivă".

68. Domeniul de aplicare a Directivei privind confidențialitatea în mediul electronic, care este în prezent limitată la furnizorii de rețele de comunicații electronice publice este unul dintre cele mai îngrijorătoare aspecte pe care propunerea nu le-a abordat. AEPD consideră că directiva ar trebui să fie modificată în sensul extinderii domeniului de aplicare pentru a include furnizorii de servicii de comunicații electronice în rețele mixte (privat/public) și în rețele private.

69. Modificările pe care AEPD le-ar prefera în mod clar nemodificate includ:

(i) **RFID**: modificarea propusă pentru *articolul 3* conform căreia rețelele de comunicații electronice includ „*rețelele de comunicații publice care presupun colectare de date și mecanisme de identificare*" este pe deplin satisfăcătoare. Această dispoziție este realmente pozitivă deoarece clarifică faptul că un număr de aplicații RFID trebuie să respecte Directiva privind confidențialitatea în mediul electronic, eliminând astfel o anumit incertitudine juridică pe marginea acestui punct.

(ii) **Cookies/spyware**: modificarea propusă pentru *articolul 5 alineatul (3)* trebuie considerată ca fiind binevenită deoarece are drept rezultat aplicarea obligației de a informa și de a da dreptul de a se opune stocării de cookies/spyware într-un echipament terminal și situației în care aceste mecanisme sunt instalate prin intermediul unor medii externe de stocare a datelor, precum CD-ROM-urile, cheile USB. Totuși, AEPD sugerează efectuarea unei modificări minore în ultima parte a articolului 5 alineatul (3), care constă în eliminarea cuvântului „a facilita" din propoziție

(iii) **Alegerea procedurii de comitologie cu consultarea AEPD și condiții/limitări aduse obligației notificării**: modificarea propusă prin care se introduce articolul 4 alineatul (4) privind notificarea încălcării securității lasă la latitudinea procedurii de comitologie, după apelarea la consiliere din partea AEPD, decizia privind chestiunile complexe referitoare la circumstanțele/formatul/procedurile sistemului de notificare a încălcării securității. AEPD sprijină pe deplin această abordare unitară. Legislația privind notificarea încălcării securității este un subiect în sine, care trebuie să fie abordat, după o dezbatere și o analiză atentă.

Legată de această chestiune este solicitarea adresată de unele părți interesate de a prevedea excepții de la obligația de a notifica încălcările securității din articolul 4 alineatul (4). AEPD se opune ferm acestei abordări. AEPD preferă ca întregul subiect al notificării, modalitățile de realizare a acesteia, precum și circumstanțele în care poate fi scurtată sau limitată notificarea să fie analizate global, după organizarea unei adevărate dezbateri.

(iv) **Punerea în aplicare**: modificarea propusă prin care se adaugă *articolul 15a* conține multe elemente utile care trebuie să fie menținute și care vor contribui la asigurarea unei respectări eficiente, inclusiv la consolidarea competențelor de investigare ale autorităților naționale de reglementare [articolul 15a alineatul (3)] și la crearea competenței autorităților naționale de reglementare de a ordona încetarea încălcărilor.

Adoptat la Bruxelles, 10 aprilie 2008.

Peter HUSTINX

Autoritatea Europeană pentru Protecția Datelor