Al doilea aviz al Autorității Europene pentru Protecția Datelor privind revizuirea Directivei 2002/58/CE privind prelucrarea datelor personale și protejarea confidențialității în sectorul comunicațiilor publice (Directiva asupra confidențialității și comunicațiilor electronice)

(2009/C 128/04)

AUTORITATEA EUROPEANĂ PENTRU PROTECȚIA DATELOR,

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

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

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

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

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

A ADOPTAT PREZENTUL AVIZ:

I. INTRODUCERE

Context

1. La 13 noiembrie 2007, Comisia Europeană a adoptat o propunere de modificare, printre altele, a Directivei asupra confidențialității și comunicațiilor electronice, de obicei denumită Directiva privind confidențialitatea în mediul electronic [1] (denumită în continuare „propunerea" sau „propunerea Comisiei"). La 10 aprilie 2008, Autoritatea Europeană pentru Protecția Datelor (AEPD) a adoptat un aviz privind propunerea Comisiei prin care prevede recomandări pentru îmbunătățirea propunerii în încercarea de a sprijini asigurarea faptului că modificările propuse au ca rezultat protejarea cât mai bună a confidențialității și a datelor cu caracter personal ale persoanelor („primul aviz al AEPD") [2].

2. AEPD a salutat propunerea Comisiei de creare a unui sistem de notificare obligatorie privind încălcarea securității care să impună societăților notificarea persoanelor în cazul în care datele cu caracter personal ale acestora au fost compromise. Mai mult, aceasta și-a manifestat aprecierea față de noua dispoziție care dă posibilitatea persoanelor juridice (de exemplu, asociațiile de consumatori și furnizorii de servicii internet) să îi acționeze în instanță pe autorii de mesaje electronice nesolicitate („spammer") și să completeze în continuare instrumentele existente de combatere a mesajelor electronice nesolicitate („spam").

3. În cursul discuțiilor parlamentare care au precedat prima lectură a Parlamentului European, AEPD a continuat să ofere consiliere prin formularea unor observații privind anumite probleme care reies din rapoartele elaborate de comitetele Parlamentului European responsabile cu revizuirea Directivei privind serviciul universal [3] și a Directivei privind confidențialitatea în mediul electronic („Observații") [4]. Observațiile au abordat, în principal, aspecte legate de prelucrarea datelor cu caracter personal și de protejarea drepturilor de proprietate intelectuală.

4. La 24 septembrie 2008, Parlamentul European („PE") a adoptat o rezoluție legislativă privind Directiva privind confidențialitatea în mediul electronic („prima lectură") [5]. AEPD a avut o opinie favorabilă cu privire la amendamentele PE care au fost adoptate ulterior avizului și observațiilor AEPD menționate anterior. Printre modificările cele mai importante s-au numărat includerea furnizorilor de servicii ale societății informaționale (și anume societățile care funcționează pe

[1] Revizuirea Directivei privind confidențialitatea în mediul electronic face parte dintr-un proces mai amplu de revizuire menit să creeze o autoritate a UE în domeniul telecomunicațiilor, să revizuiască Directivele 2002/21/CE, 2002/19/CE, 2002/20/CE, 2002/22/CE și 2002/58/CE, precum și Regulamentului (CE) nr. 2006/2004 (denumit în continuare „revizuirea pachetului telecomunicații").

[2] 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 asupra confidențialității și comunicațiilor electronice), JO C 181, 18.7.2008, p. 1.

[3] Directiva 2002/22/CE privind serviciile universale și drepturile utilizatorilor cu privire la rețelele și serviciile electronice de comunicații (Directiva privind serviciul universal), JO L 108, 24.4.2002, p. 51.

[4] Observațiile AEPD privind anumite probleme care reies din raportul IMCO privind revizuirea Directivei 2002/22/CE (Directiva privind serviciul universal) & Directiva 2002/58/CE (Directiva privind confidențialitatea în mediul electronic), 2 septembrie 2008. Disponibile la adresa de internet: www.edps.europa.eu

[5] Rezoluția legislativă a Parlamentului European din 24 septembrie 2008 privind 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 [(COM(2007)0698 - C6-0420/2007 - 2007/0248(COD)].

internet) în domeniul de aplicare a obligației de notificare a încălcărilor securității. AEPD a salutat, de asemenea, amendamentul care dă posibilitatea persoanelor fizice și juridice să acționeze în justiție pentru încălcarea oricărei dispoziții a Directivei privind confidențialitatea în mediul electronic (nu numai pentru violarea dispozițiilor privind „spam"-ul, cum propunea inițial propunerea Comisiei). Prima lectură a Parlamentului a fost urmată de adoptarea de către Comisie a unei propuneri modificate privind Directiva privind confidențialitatea în mediul electronic (denumită în continuare „propunerea modificată") ([6]).

5. La 27 noiembrie 2008, Consiliul a ajuns la un acord politic cu privire la revizuirea normelor privind pachetul telecomunicații, inclusiv Directiva privind confidențialitatea în mediul electronic, care va deveni poziția comună a Consiliului („poziția comună") ([7]). Poziția comună va fi comunicată PE în temeiul articolului 251 alineatul (2) din Tratatul de instituire a Comunității Europene, care este posibil să atragă după sine propuneri de amendamente ale PE.

Opinii cu caracter general privind poziția Consiliului

6. Consiliul a modificat elemente esențiale ale textului propunerii și nu a acceptat multe dintre amendamentele adoptate de PE. Deși poziția comună conține cu siguranță elemente pozitive, în general, AEPD își exprimă preocuparea față de conținutul acesteia, în special deoarece poziția comună nu include unele dintre amendamentele pozitive propuse de PE, de propunerea modificată sau de avizele AEPD și ale autorităților europene de protecție a datelor emise prin intermediul Grupului de lucru „articolul 29" ([8]).

7. Pe de altă parte, într-un număr semnificativ de cazuri, unele dispoziții prevăzute de propunerea modificată și de amendamentele PE, care oferă cetățenilor garanții de protecție, sunt eliminate sau diluate în mod substanțial. Ca rezultat, nivelul de protecție acordat persoanelor prin poziția comună este diminuat în mod substanțial. Din aceste motive, AEPD emite acum un al doilea aviz în speranța că, în timp ce Directiva privind confidențialitatea în mediul electronic își continuă parcursul în cadrul procesului legislativ, vor fi adoptate noi amendamente care vor restabili garanțiile de protecție a datelor.

8. Prezentul al doilea aviz se concentrează asupra unor preocupări esențiale și nu repetă nici toate argumentele din cadrul primului aviz al AEPD, nici observațiile, care rămân în întregime valabile. Prezentul aviz discută, în special, următoarele aspecte:

— dispozițiile referitoare la notificarea încălcării securității;

— domeniului de aplicare a Directivei privind confidențialitatea în mediul electronic în cazul rețelelor private și al rețelelor private accesibile publicului;

— prelucrarea datelor de trafic în scopuri de securitate;

— posibilitatea persoanelor juridice de a intenta o acțiune în justiție în cazul încălcării oricărei dispoziții a Directivei privind confidențialitatea în mediul electronic.

9. În abordarea aspectelor sus-menționate, prezentul aviz analizează poziția comună a Consiliului și o compară cu prima lectură a PE și cu propunerea modificată a Consiliului. Avizul include recomandări menite să simplifice dispozițiile Directivei privind confidențialitatea în mediul electronic și să se asigure că directiva continuă să protejeze în mod adecvat confidențialitatea și datele cu caracter personal ale persoanelor.

II. DISPOZIȚIILE REFERITOARE LA NOTIFICAREA ÎNCĂLCĂRII SECURITĂȚII

10. AEPD sprijină adoptarea unui sistem de notificare a încălcărilor securității potrivit căruia autoritățile și persoanele vor fi notificate atunci când datele cu caracter personal ale acestora au fost compromise ([9]). Notificările încălcărilor securității pot ajuta persoanele să ia măsurile necesare pentru diminuarea potențialelor prejudicii rezultate în urma compromiterii datelor. În plus, obligația de a trimite notificări care să informeze cu privire la încălcările securității vor încuraja societățile să-și îmbunătățească securitatea datelor și să-și sporească responsabilitatea cu privire la datele cu caracter personal de care răspund.

11. Propunerea modificată a Comisiei, prima lectură a Parlamentului European și poziția comună a Consiliului reprezintă trei abordări diferite ale notificării încălcărilor securității aflate actualmente în discuție. Fiecare dintre cele trei abordări are aspecte pozitive. Cu toate acestea, AEPD crede că rămâne loc pentru îmbunătățiri în fiecare dintre abordări și recomandă să se țină seama de recomandările prezentate mai jos la stabilirea etapelor finale către adoptarea unui sistem de notificare a încălcărilor securității.

([6]) Propunere modificată 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, 6.11.2008, COM(2008) 723 final.

([7]) Disponibilă pe site-ul public al Consiliului.

([8]) Avizul 2/2008 privind revizuirea Directivei 2002/58/CE asupra confidențialității și comunicațiilor electronice (Directiva privind confidențialitatea în mediul electronic), disponibil pe site-ul Grupului de lucru „articolul 29".

([9]) Prezentul aviz utilizează termenul „compromis" pentru a se referi la orice violare a datelor cu caracter personal care a avut loc ca urmare a distrugerii accidentale sau ilegale, a pierderii, alterării, divulgării neautorizate sau accesului neautorizat la datele cu caracter personal transmise, stocate sau prelucrate în alt mod.

12. La analizarea celor trei sisteme de notificare a încălcărilor securității, trebuie analizate cinci aspecte de importanță majoră: (*i*) definiția unei încălcări a securității; (*ii*) entitățile care intră sub incidența obligației de notificare („entități reglementate"); (*iii*) standardul care conduce la obligația de notificare; (*iv*) identificarea entității responsabile să stabilească dacă o încălcare a securității îndeplinește sau nu standardul, și (v) destinatarii notificării.

Prezentare generală a abordărilor Comisiei, Consiliului și Parlamentului European

13. Parlamentul European, Comisia și Consiliul au adoptat fiecare diferite abordări pentru notificarea încălcărilor securității. Prima lectură a PE a modificat sistemul inițial de notificare a încălcărilor securității prezentat de propunerea Comisiei ([10]). Potrivit abordării PE, obligația de notificare se aplică nu numai furnizorilor de servicii de comunicații electronice accesibile publicului, ci și furnizorilor de servicii ai societății informaționale („FSCEP" și „FSSI"). În plus, potrivit acestei abordări, toate violările datelor cu caracter personal vor trebui să fie comunicate autorității naționale de reglementare sau autorităților competente (denumite împreună „autoritățile"). Dacă autoritățile ar determina că violarea este *gravă*, acestea ar impune FSCEP și FSSI să notifice fără întârziere persoana. În cazul unor violări care reprezintă un pericol iminent și direct, FSCEP și FSSI ar notifica persoanele înainte de notificarea autorităților și nu ar aștepta o hotărâre de reglementare. O derogare de la obligația de notificare a consumatorilor are ca obiect entitățile care pot demonstra autorităților că *„s-au aplicat măsurile adecvate de protecție tehnică"* care fac datele ininteligibile pentru orice persoană care nu are acces autorizat la acestea.

14. Potrivit abordării Consiliului, notificarea trebuie, de asemenea, să fie asigurată atât abonaților, cât și autorităților, dar numai în cazurile în care *entitățile reglementate* consideră că violarea reprezintă un *risc grav* la adresa confidențialității abonatului (și anume furtul sau frauda de identitate, vătămări fizice, umilința gravă sau compromiterea reputației).

15. Propunerea modificată a Comisiei menține obligația PE de a notifica autoritățile în cazul tuturor violărilor. Cu toate acestea, spre deosebire de abordarea PE, propunerea modificată include o derogare de la cerința de notificare a persoanele vizate în cazul în care furnizorul de servicii de comunicații electronice (FSCE) demonstrează autorității competente că (i) este *„destul de puțin probabil"* ca violarea datelor cu caracter personal să conducă la prejudicii (de exemplu pagube de ordin economic, prejudicii sociale sau furtul de identitate) sau (ii) datelor compromise li s-au aplicat *„măsuri adecvate de protecție tehnologică"*. Astfel, abordarea Comisiei include o analiză bazată pe prejudicii în conexiune cu notificările persoanelor.

([10]) În special amendamentele PE nr. 187, 124 și 127, precum și 27, 21 și 32 abordează acest aspect.

16. Este important de remarcat că, potrivit abordărilor PE ([11]) și a Comisiei, *autoritățile* sunt cele care, în ultimă instanță, sunt însărcinate să stabilească dacă violarea este gravă sau dacă este destul de probabil ca aceasta să aducă prejudicii. Din contră, potrivit abordării Consiliului, decizia rămâne la latitudinea *autorităților vizate*.

17. Atât abordarea Consiliului, cât și a Comisiei, se aplică numai FSCEP, nu și FSSI, ca în cazul abordării PE.

Definiția încălcării securității

18. AEPD își exprimă satisfacția cu privire la faptul că cele trei propuneri legislative conțin aceeași definiție a notificării încălcărilor securității, care este descrisă ca *„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 […]"* ([12]).

19. Astfel cum se descrie în continuare, această definiție este binevenită deoarece aceasta este suficient de amplă încât să cuprindă majoritatea situațiilor relevante în care notificarea încălcărilor securității ar putea fi justificată.

20. În primul rând, această definiție include situațiile în care o parte terță a avut *acces neautorizat* la date cu caracter personal, cum ar fi hacking-ul unui server care conține date cu caracter personal și extragerea de astfel de informații.

21. În al doilea rând, această definiție ar include, de asemenea, situațiile în care s-a înregistrat o pierdere sau divulgarea de date cu caracter personal, iar accesul neautorizat nu a fost încă dovedit. Aceasta ar include situațiile în care este posibilă pierderea unor date cu caracter personal (de exemplu CD-ROM-uri, memorii USB sau alte tipuri de memorii portabile), sau punerea la dispoziția publicului a unor astfel de date de către utilizatorii obișnuiți (fișiere de date cu caracter personal ale angajaților puse din neatenție sau temporar la dispoziția publicului prin intermediul internetului). Deoarece deseori nu vor exista dovezi care să demonstreze că astfel de date pot sau nu pot, la una moment dat, fi accesate sau utilizate de părți terțe neautorizate, pare adecvată includerea acestor situații în domeniul de aplicare al definiției. Prin urmare, AEPD recomandă menținerea acestei definiții. AEDP recomandă, de asemenea, includerea definiției încălcării securității în articolul 2 din Directiva privind confidențialitatea în mediul electronic, deoarece aceasta ar fi mai compatibilă cu structura generală a directivei și ar oferi mai multă claritate.

([11]) Cu excepția cazurilor de pericol iminent și direct, caz în care entitățile vizate trebuie să notifice mai întâi consumatorii.

([12]) Articolul 2 punctul (i) din poziția comună și din propunerea modificată și articolul 3 alineatul (3) din prima lectură a PE.

Entități care ar trebui să intre sub incidența obligației de notificare

22. Potrivit abordării PE, obligația de notificare se aplică atât FSCEP, cât și FSSI. Pe de altă parte, în cadrul sistemelor Consiliului și Comisiei, numai FSCEP cum ar fi companiile de telecomunicații și furnizorii de acces la internet vor avea obligația să notifice persoanele în cazul unor încălcări ale securității care au ca rezultat compromiterea unor date cu caracter personal. Alte sectoare de activitate, de exemplu băncile online, comercianții cu amănuntul online, furnizorii de servicii medicale online și alții nu sunt supuși acestei obligații. Din motivele prezentate mai jos, AEDP consideră că din punctul de vederea al unei politici publice este critică asigurarea faptului că serviciile societății informaționale care includ afaceri online, bănci online, furnizori de servicii medicale online etc. intră, de asemenea, sub incidența obligației de notificare.

23. În primul rând, AEPD constată că, deși companiile de telecomunicații sunt, desigur, ținta încălcărilor securității care justifică obligația notificării, acest lucru este valabil și pentru alte tipuri de societăți/furnizori. Comercianții cu amănuntul online, băncile online, farmaciile online sunt la fel de expuși riscului de a suferi încălcări ale securității ca și companiile de telecomunicații, dacă nu chiar în măsură și mai mare. Prin urmare, evaluarea riscurilor nu înclină balanța în favoarea limitării domeniului de aplicare al cerinței de notificare a încălcărilor securității numai la FSCEP. Necesitatea unei abordări mai largi este ilustrată de experiența altor țări. De exemplu, în Statele Unite ale Americii aproape toate statele (mai mult de 40 în această situație) au adoptat legi privind notificarea încălcărilor securității care au un domeniu de aplicare mai larg, cuprinzând nu numai FSCEP, ci și orice entitate care deține datele cu caracter personal solicitate.

24. În al doilea rând, în timp ce orice violare a tipurilor de date cu caracter personal prelucrate în mod regulat de către FSCEP poate avea, în mod clar, impact asupra confidențialității persoanelor, același lucru este valabil, dacă nu chiar într-o măsură și mai mare, și în cazul tipurilor de informații personale procesate de FSSI. Băncile și alte instituții financiare pot fi, desigur, în posesia unor informații cu grad înalt de confidențialitate (de exemplu date privind conturile bancare), a căror divulgare poate servi în scopuri de furt al identității. De asemenea, divulgarea unor informații foarte sensibile cu privire la sănătate de către serviciile medicale online poate fi deosebit de dăunătoare persoanelor. Prin urmare, tipurile de date cu caracter personal care pot fi compromise necesită, de asemenea, o aplicare mai largă a notificării încălcărilor securității care ar include cel puțin FSSI.

25. S-au semnalat unele probleme juridice împotriva extinderii domeniului de aplicare al prezentului articol, și anume cu privire la entitățile care intră sub incidența acestei obligații. În mod deosebit, faptul că domeniul de aplicare general al Directivei privind confidențialitatea în mediul electronic vizează numai FSCEP a fost semnalat ca un obstacol în calea aplicării obligației notificării și furnizorilor de servicii ale societăți informaționale.

26. În acest context, AEPD ar dori să reamintească următoarele: *(i)* Nu există niciun obstacol juridic care să împiedice includerea altor actori în afara FSCEP în domeniul de aplicare al anumitor dispoziții din directivă. Legiuitorul comunitar dispune de libertate totală în această privință. *(ii)* Există și alte precedente în Directiva privind confidențialitatea în mediul electronic existentă privind aplicarea în cazul altor entități în afara FSCEP.

27. De exemplu, articolul 13 se aplică nu numai FSCEP, ci și oricărei societăți care trimite informații nesolicitate, necesitând consimțământ prealabil pentru aceasta. În plus, articolul 5 alineatul (3) din Directiva privind confidențialitatea în mediul electronic, care interzice, printre altele, stocarea informațiilor cum ar fi cookies în echipamentul terminal al utilizatorilor, are caracter obligatoriu nu numai pentru FSCEP, ci și pentru oricine încearcă să stocheze informații sau să obțină acces la informații stocate în echipamentul terminal al persoanelor. În plus, în procesul legislativ actual, Comisia a propus extinderea aplicării articolului 5 alineatul (3) în cazul în care tehnologii similare (cookies/spyware) sunt distribuite nu numai prin intermediul sistemelor de comunicații electronice, ci și prin orice altă metodă posibilă (distribuire prin descărcări de pe internet sau prin intermediul mediilor externe de stocare a datelor, cum ar CD-ROM-urile, cheile USB, flash drive-urile etc.). Toate aceste elemente sunt binevenite și ar trebui nu numai să fie păstrate, ci și să creeze precedente relevante pentru prezenta discuție cu privire la domeniul de aplicare.

28. În plus, în cadrul procesului legislativ actual, Comisia, PE și se poate spune că și Consiliul au propus un nouă versiune a articolului 6 alineatul 6 litera (a), discutată mai jos, care se aplică altor entități în afara FSCEP.

29. În cele din urmă, ținând seama de elementele pozitive cuprinzătoare derivate din obligația notificării încălcărilor de securitate, este foarte probabil ca cetățenii să se aștepte la aceste beneficii nu numai atunci când datele cu caracter personal au fost compromise de către FSCEP, ci și în cazul FSSI. Este posibil ca așteptările cetățenilor să nu fie îndeplinite dacă, de exemplu, aceștia nu sunt notificați în cazul în care o bancă online a pierdut informațiile acestora privind conturile bancare.

30. Pe scurt, AEPD este convinsă că beneficiile depline ale notificării încălcărilor securității vor fi mai bine obținute numai dacă domeniul de aplicare al entităților reglementate va include atât FSCEP, cât și FSSI.

Standardul care conduce la obligația de notificare

31. În ceea ce privește elementul declanșator al notificării, astfel cum se explică în continuare, AEDP este de părere că standardul propunerii modificate, care include criteriul „*este destul de probabil să aducă prejudicii*", reprezintă varianta cea mai adecvată dintre cele trei standarde propuse. Cu toate acestea, este important să se asigure faptul că „prejudicii" este un termen suficient de amplu încât să cuprindă toate situațiile de efecte negative asupra confidențialității sau asupra altor interese legitime ale persoanelor. În caz contrar, ar fi de preferat să se creeze un nou standard potrivit căruia notificarea să fie obligatorie „dacă *este destul de probabil ca încălcarea să aibă efecte nefavorabile asupra persoanelor*".

32. Astfel cum s-a subliniat în secțiunea precedentă, condițiile în care notificarea persoanelor trebuie efectuată (denumite „elementul declanșator" sau „standardul") sunt diferite în abordările PE, a Comisiei și a Consiliului. În mod evident, volumul notificărilor pe care le vor primi persoanele va depinde, în mare parte, de elementul declanșator sau de standardul stabilit pentru notificare.

33. Potrivit sistemelor Consiliului și Comisiei, notificarea trebuie efectuată dacă încălcarea reprezintă o „*încălcare gravă la adresa confidențialității abonatului*" (Consiliul) și dacă „*este destul de probabil ca încălcarea să aibă ca rezultat prejudicii aduse intereselor consumatorilor*" (Comisia). Potrivit sistemului Parlamentului European, elementul declanșator al notificării persoanelor este „*gravitatea încălcării*" (adică notificarea persoanelor este necesară dacă încălcarea este considerată „*gravă*"). Notificarea nu este necesară dacă acest prag nu a fost atins ([13]).

34. AEPD înțelege că, dacă au fost compromise date cu caracter personal, se poate susține că persoanele cărora le aparțin datele au dreptul să afle, în orice situație, acest lucru. Cu toate acestea, ținând seama de alte interese și considerații, este corect să se analizeze atent dacă aceasta este o soluție adecvată.

35. S-a sugerat că obligația de a trimite notificări ori de câte ori au fost compromise date cu caracter personal, cu alte cuvinte fără nicio limitare, poate conduce la notificare exagerată și la o „oboseală a notificării", care ar avea ca rezultat desensibilizarea. Astfel cum se descrie în continuare, AEPD este sensibilă la acest argument; cu toate acestea, AEPD dorește să-și sublinieze preocuparea față de notificarea exagerată ca posibil indicator al unui eșec larg răspândit al practicilor din domeniul securității informațiilor.

36. Așa cum s-a menționat anterior, AEPD a remarcat potențialele consecințe negative ale notificării exagerate și ar dori să contribuie la asigurarea faptului că adoptarea cadrului legal pentru notificarea încălcărilor securității nu produce acest rezultat. Dacă persoanele ar primi notificări frecvente ale încălcării, chiar și în situații în care nu există efecte nefavorabile, prejudicii sau pericol, este posibil să se ajungă la subminarea unuia din scopurile-cheie ale notificării, deoarece, în mod ironic, persoanele pot să ignore notificările în acele situații în care ar putea fi necesar să ia măsuri să se protejeze. Așadar este important să se găsească echilibrul potrivit în efectuarea notificărilor deoarece, dacă persoanele nu reacționează la notificările primite, eficacitatea sistemelor de notificare va fi semnificativ redusă.

37. Pentru a adopta un standard adecvat care să nu conducă la notificare exagerată, trebuie să se țină seama, în afara elementului declanșator al notificării, și de alți factori, în special de definiția încălcărilor securității și de informația care face obiectul obligației de notificare. În această privință, AEPD constată că potrivit celor trei abordări propuse, volumul notificărilor poate fi ridicat dacă se ține seama de definiția extinsă a încălcărilor securității discutată anterior. Această preocupare față de notificarea exagerată evidențiată în continuare de faptul că definiția încălcărilor securității are ca obiect toate tipurile de date cu caracter personal. Deși AEPD consideră că aceasta este abordarea corectă (fără a limita tipul de date cu caracter personal care fac obiectul notificării), spre deosebire de alte abordări, cum ar fi cea a legislației USA, în care obligațiile se concentrează asupra sensibilității informațiilor, notificarea exagerată constituie, totuși, un factor de care să se țină seama.

38. În lumina celor sus-menționate, și luând în considerare diferitele variabile luate în ansamblu, AEPD consideră adecvat să includă un prag sau un standard sub nivelul căruia notificarea să nu fie obligatorie.

39. Ambele standarde propuse, și anume faptul că încălcarea reprezintă un „*risc* grav *la adresa confidențialității*" sau că este „*destul de probabil să aducă prejudicii*" par să includă, de exemplu, prejudicii sociale sau în privința reputației și pagube economice. De exemplu, aceste standarde ar aborda situațiile de expunere la furtul de identitate prin divulgarea de identificatori care nu sunt puși la dispoziția publicului cum ar fi numerele pașapoartelor, precum și dezvăluirea de informații cu privire la viața personală a persoanelor. AEPD salută această abordare. Aceasta este convinsă că beneficiile notificării încălcărilor securității nu ar fi pe deplin obținute dacă sistemul de notificare ar avea ca obiect numai încălcările care au ca rezultat pagube economice.

([13]) A se vedea nota de subsol 11 privind excepția de la această regulă.

40. Dintre cele două standarde propuse, AEPD preferă standardul Comisiei, „*este destul de probabil să aducă prejudicii*”, deoarece acesta ar oferi un nivel de protecție a persoanelor mai adecvat. Este de departe mult mai probabil ca încălcările să se califice pentru notificare dacă este „*destul de probabil ca acestea să aducă prejudicii*” decât dacă reprezintă un „*risc grav*” la adresa confidențialității persoanelor. Astfel, reducerea reglementării numai la încălcările care prezintă un risc grav la adresa confidențialității persoanelor ar limita considerabil numărul de încălcări care trebuie notificate. Reducerea reglementării numai la astfel de încălcări ar da o libertate prea mare FSCEP și FSSI în stabilirea necesității unei notificări, în măsura în care ar fi mult ușor pentru aceștia să justifice concluzia că nu există niciun „*risc grav*” de prejudiciu, decât că este „*destul de probabil să nu se aducă*” niciun prejudiciu. În timp ce notificările exagerate trebuie, desigur, evitate, pentru a avea echilibru trebuie acordat beneficiul îndoielii protejării intereselor de confidențialitate ale persoanelor, iar persoanele ar trebui să fie protejate cel puțin în situația în care este destul de probabil ca o încălcare să le aducă prejudicii. Mai mult, expresia „*destul de probabil*” va fi mai eficace în practică, atât în cazul entităților reglementate, cât și în cazul autorităților competente, deoarece impune o evaluare obiectivă a situației și a contextului relevant al acesteia.

41. În plus, violările datelor cu caracter personal pot aduce prejudicii care sunt dificil de cuantificat și care pot fi de natură diferită. Într-adevăr, dezvăluirea aceluiași tip de date, în funcție de circumstanțele individuale, pot provoca prejudicii semnificative unei persoane și în mai mică măsură alteia. Un standard care ar impune ca prejudiciul să fie de natură materială, semnificativ sau grav, nu ar fi adecvat. De exemplu, abordarea Consiliului, care impune ca încălcarea să aducă *grav* atingere confidențialității cuiva, ar asigura protecție inadecvată persoanelor în măsura în care un astfel de standard impune ca efectul asupra confidențialității să fie „grav”. Aceasta lasă loc, de asemenea, unei evaluări subiective.

42. Cu toate că, astfel cum s-a descris anterior, „*destul de probabil să aducă prejudicii*” pare să fie un standard adecvat pentru notificarea unei încălcării a securității, AEDP rămâne preocupată de faptul că acesta ar putea să nu includă toate situațiile în care notificarea persoanelor este justificată, de exemplu toate situațiile în care efecte negative asupra confidențialității sau asupra altor drepturi legitime ale persoanelor sunt destul de probabile. Din acest motiv, ar putea fi luat în considerare un standard care să impună notificare „*dacă este destul de probabil ca încălcarea să aibă efecte nefavorabile*”.

43. Acest standard alternativ are avantajul suplimentar al coerenței cu legislația UE privind protecția datelor. Într-adevăr, Directiva privind protecția datelor se referă adesea la efectele nefavorabile asupra drepturilor și libertăților persoanelor vizate. De exemplu, articolul 18 și considerentul 49, care fac referire la obligația de a înregistra operațiunile de prelucrare a datelor la autoritățile de protecție a datelor autorizează statele membre să facă derogare de la această obligație în cazurile în care prelucrarea „*nu poate aduce atingere drepturilor și libertăților persoanelor vizate*”. O formulare similară este utilizată la articolul 16 alineatul (6) din poziția comună pentru a da posibilitatea peroanelor juridice să acționeze în justiție împotriva spammer-ilor.

44. Mai mult, ținând seama de cele sus-menționate, s-ar putea preconiza, de asemenea, ca entitățile reglementate și, în special, autoritățile responsabile cu aplicarea legislației privind protecția datelor să cunoască mai bine standardul menționat anterior și astfel să-și ușureze evaluarea prin care stabilesc dacă o anumită încălcare îndeplinește sau nu standardul cerut.

Entitatea care determină dacă o încălcare a securității îndeplinește sau nu standardul

45. Potrivit abordării PE (cu excepția cazurilor de pericol iminent) și propunerii modificate a Comisiei, va rămâne la latitudinea autorităților statelor membre să determine dacă o încălcare a securității îndeplinește sau nu standardul care declanșează obligația de notificare a persoanelor vizate.

46. AEPD consideră că implicarea unei autorități joacă un rol important în a determina dacă standardul este îndeplinit în măsura în care, acesta reprezintă, într-o oarecare măsură, o garanție pentru aplicarea corectă a legii. Un astfel de sistem poate evita situația în care societățile evaluează încălcarea ca nefiind gravă/serioasă și astfel evită notificarea deși, de fapt, notificarea este necesară.

47. Pe de altă parte, AEPD își manifestă preocuparea că un regim prin care autorităților li se impune să efectueze evaluarea ar putea fi imposibil în practică sau greu de aplicat, sau se poate dovedi contraproductiv în practică. Astfel s-ar putea chiar diminua garanțiile de protecție a datelor pentru persoane.

48. Într-adevăr, potrivit unei astfel de abordări, este posibil ca autoritățile de protecție a datelor să fie inundate cu notificări de încălcări ale securității și să fie confruntate cu dificultăți serioase în efectuarea evaluărilor necesare. Este important să reamintim că pentru a efectua evaluarea dacă o încălcare îndeplinește standardul, autorităților vor trebui să li se asigure suficiente informații din interior, deseori de natură tehnică complexă, pe care vor trebui să le prelucreze foarte repede. Ținând seama de dificultatea evaluării și de faptul că unele autorități au resurse limitate, AEPD își manifestă teama că va fi dificil pentru autorități să respecte această obligație și că aceasta va prelua resurse de la alte priorități importante. În plus, un astfel de sistem ar putea exercita o presiune nejustificată asupra autorităților; într-adevăr, dacă autoritățile au decis că încălcarea nu este gravă și, cu toate acestea, persoanele suferă prejudicii, autoritățile ar putea fi trase la răspundere.

49. Dificultatea sus-menționată este subliniată mai mult dacă se ține seama că timpul este un factor-cheie în reducerea riscurilor derivate din încălcări ale securității. Dacă autoritățile nu reușesc să efectueze evaluarea în termene foarte scurte, răstimpul suplimentar necesar autorităților în efectuarea evaluărilor poate spori prejudiciile suferite de persoanele vizate. Prin urmare, această măsură suplimentară, menită să asigure o protecție sporită persoanelor, poate, în mod ironic, să aibă ca rezultat asigurarea unei protecții mai reduse decât sistemele bazate pe notificarea directă.

50. Din motivele sus-menționate, AEPD consideră că ar fi preferabilă instituirea unui sistem prin care ar trebui să rămână la latitudinea entităților vizate să facă evaluarea dacă o încălcare îndeplinește sau nu standardul, astfel cum prevede abordarea Consiliului.

51. Cu toate acestea, pentru a evita riscurile de abuz, de exemplu refuzul entităților de a notifica în circumstanțe în care notificarea este în mod clar necesară, este deosebit de important să se includă anumite garanții de protecție a datelor prezentate în continuare.

52. În primul rând, obligația care revine entităților reglementate de a stabili dacă trebuie să notifice trebuie să fie însoțită de o altă obligație prin care se impune autorităților notificarea obligatorie a tuturor încălcărilor care îndeplinesc standardul cerut. Entitățile vizate ar trebui, în acele cazuri, să fie obligate să informeze autoritățile cu privire la încălcare și la motivele evaluării privind notificarea, precum și la conținutul oricărei notificări efectuate.

53. În al doilea rând, autorităților trebuie să li se dea un rol de supraveghere veritabil. În exercitarea acestui rol, autoritățile trebuie să aibă permisiunea, dar să nu fie obligate, să investigheze circumstanțele încălcării și să solicite orice măsuri de remediere pe care le consideră adecvate ([14]). Acesta ar trebui să includă nu numai notificarea persoanelor (în cazul în care acesta nu a fost deja efectuată), ci și competența de a impune obligația de a lua măsuri pentru prevenirea altor încălcări. Autorităților ar trebui să li se acorde competențe și resurse efective în această privință și trebuie să aibă marja de manevră necesară pentru a decide când să reacționeze la o notificare a unei încălcări a securității. Cu alte cuvinte, aceasta ar da autorităților posibilitatea să fie selective și să înceapă investigații cu privire la, de exemplu, încălcări de anvergură ale securității, care aduc prejudicii cu adevărat grave, verificând și asigurând respectarea cerințelor legii.

54. Pentru a realiza cele sus-menționate, pe lângă competențele recunoscute în temeiul Directivei privind confidențialitatea în mediul electronic, cum ar fi articolul 15a alineatul (3), și al Directivei privind protecția datelor, AEPD recomandă inserarea următoarea formulări: „*Dacă abonatul sau persoana vizată nu a fost deja notificată, autoritatea națională competentă, în urma analizării naturii încălcării, poate solicita FSCEP sau FSSI să efectueze notificarea*”.

55. În plus, AEPD recomandă PE și Consiliului să confirme obligația propusă de PE [amendamentul 122, articolul 4 alineatul (1) litera (a)] ca entitățile să efectueze o evaluare și o identificare a riscurilor privind sistemele lor și datele cu caracter personal pe care intenționează să le prelucreze. Pe baza acestei obligații, entitățile elaborează o definiție adaptată și precisă a măsurilor de securitate care vor fi aplicate în cazurile lor și care ar trebui să fie puse la dispoziția autorităților. Dacă se produce o încălcare a securității, această obligație va ajuta entitățile reglementate – și, în cele din urmă, și autoritățile în rolul lor de supraveghere – să determine dacă compromiterea informațiilor poate cauza efecte nefavorabile sau prejudicii la adresa persoanelor.

56. În al treilea rând, obligația aplicabilă entităților reglementate de a determina dacă trebuie să notifice persoanele trebuie însoțită de obligația de a înregistra un parcurs de audit intern detaliat și cuprinzător care să descrie toate încălcările care au avut loc și toate notificările acestora, precum și orice măsuri întreprinse pentru evitarea încălcărilor viitoare. Acest parcurs de audit intern trebuie să fie pus la dispoziția autorităților pentru examinare și o posibilă investigație. Aceasta va permite autorităților să-și exercite rolul de supraveghere. Aceasta se va putea realiza prin adoptarea unei formulări de tipul următor: „*FSCEP și FSSI țin și actualizează o evidență cuprinzătoare care să prezinte în detaliu toate încălcările care au avut loc, informațiile tehnice relevante conexe și măsurile de remediere adoptate. Evidența face, de asemenea, referire la toate notificările emise abonaților sau persoanelor vizate și autorităților naționale competente, inclusiv data și conținutul acestora. Evidența este prezentată autorității naționale competente la cererea acesteia.*”

57. Desigur, pentru a asigura coerență în implementarea acestui standard, precum și alte aspecte relevante ale cadrului încălcării securității, cum ar fi formatul și procedurile de notificare, ar fi adecvat ca Comisia să ia măsurile de implementare tehnică, în urma consultării cu AEPD, Grupul de lucru „articolul 29” și cu părțile interesate relevante.

([14]) Articolul 15a alineatul (3) recunoaște aceste competențe de supraveghere prin faptul că prevede că „Statele membre se asigură că autoritățile naționale competente și, atunci când este cazul, alte organisme naționale, dețin toate drepturile de investigație și resursele necesare, inclusiv posibilitatea de a obține orice informație relevantă care s-ar putea dovedi necesară în vederea monitorizării și aplicării dispozițiilor naționale adoptate în temeiul prezentei directive.”

Destinatarii notificării

58. În ceea ce privește destinatarii notificării, AEPD preferă terminologia PE și a Comisiei în detrimentul celei a Consiliului. Într-adevăr, PE a înlocuit termenul „abonați" cu expresia „utilizatori". Comisia utilizează „abonați" și „persoane vizate". Atât limbajul PE, cât și al Comisiei ar include ca destinatari ai notificărilor nu numai abonații actuali, ci și foști abonați și părți terțe, cum ar fi utilizatorii care interacționează cu unele entități reglementate fără să se aboneze la acestea. AEPD salută această abordare și face apel către PE și Consiliu să o mențină.

59. Cu toate acestea, AEPD constată un număr de inconsecvențe cu privire la terminologia din prima lectură a PE care ar trebui remediate. De exemplu, termenul „abonați" a fost înlocuit în majoritatea cazurilor, dar nu în toate, cu expresia „utilizatori", iar în alte cazuri cu termenul „consumatori". Aceștia ar trebui armonizați.

III. DOMENIUL DE APLICARE AL DIRECTIVEI PRIVIND CONFIDENȚIALITATEA ÎN MEDIUL ELECTRONIC: REȚELELE PUBLICE ȘI PRIVATE

60. Articolul 3 alineatul (1) din actuala Directivă privind confidențialitatea în mediul electronic stabilește entitățile vizate în primul rând de către directivă, și anume acelea care prelucrează date „*legate de*" furnizarea de servicii de comunicații electronice publice prin intermediul rețelelor publice (la care se face referire anterior sub denumirea de „FSCEP") ([15]). 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.

61. PE a adoptat amendamentul 121 de modificare a articolului 3 din propunerea inițială a Comisiei, în temeiul căruia domeniul de aplicare al Directivei privind confidențialitatea în mediul electronic a fost extins pentru a include „*prelucrarea de date personale legate de furnizarea de servicii de comunicații electronice accesibile publicului prin intermediul rețelelor publice și private de comunicații electronice și al rețelelor private accesibile publicului din cadrul Comunității, […]*" [articolul 3 alineatul (1) din Directiva privind confidențialitatea în mediul electronic]. Din păcate, Consiliul și Comisia nu au putut accepta acest amendament și prin urmare nu au inclus această abordare în poziția comună și nici în propunerea modificată.

Aplicarea Directivei privind confidențialitatea în mediul electronic la rețelele private accesibile publicului

62. Din motivele explicate mai jos și pentru a sprijini ajungerea la un consens, AEPD încurajează menținerea elementelor esențiale ale amendamentului 121. În plus, AEPD sugerează includerea unui amendament care să clarifice mai bine tipurile de servicii care ar fi incluse în domeniul de aplicare extins.

63. Rețelele private sunt deseori utilizate pentru a oferi servicii de comunicații electronice, cum ar fi accesul la internet, unui număr nedefinit de persoane, care ar putea fi ridicat. Acesta este, de exemplu, cazul accesului la internet în cafenelele internet, precum și spațiile WiFi disponibile în hoteluri, restaurante, aeroporturi, trenuri și în alte instituții deschise publicului unde astfel de servicii sunt deseori furnizate în completarea altor servicii (băuturi, cazare etc.).

64. În toate exemplele anterioare, un serviciu de comunicații, de exemplu accesul la internet, este pus la dispoziția publicului nu prin intermediul unei rețele publice, ci mai curând prin ceea ce poate fi considerat o rețea privată, adică o rețea care funcționează într-un spațiu privat. Mai mult, deși în cazurile descrise anterior, serviciile de comunicații sunt furnizate publicului, deoarece tipul de rețea utilizată este mai curând privat decât public, s-ar putea spune că aceste servicii nu sunt reglementate de întreaga Directivă privind confidențialitatea în mediul electronic sau cel puțin de unele din articolele acesteia ([16]). Ca urmare, drepturile fundamentale ale persoanelor garantate de Directiva privind confidențialitatea în mediul electronic nu sunt protejate în aceste situații și se creează o situație juridică inegală pentru utilizatorii care recurg la aceleași servicii de acces la internet prin mijloace de telecomunicații publice față de cei care recurg la acestea prin mijloace private. Aceasta în ciuda faptului că riscurile privind confidențialitatea și datele cu caracter personal în toate aceste cazuri există în același grad ca și în cazul în care sunt utilizate rețele publice pentru furnizarea serviciilor. Pe scurt, se pare că nu există niciun motiv care să justifice, în temeiul Directivei, tratamentul diferențiat al serviciilor de comunicații furnizate printr-o rețea privată față de cele furnizate printr-o rețea publică.

65. Prin urmare, AEPD ar sprijini un amendament, cum ar fi amendamentul 121 ale PE, în temeiul căruia Directiva privind confidențialitatea în mediul electronic s-ar aplica și prelucrării datelor cu caracter personal coroborate cu furnizarea de servicii de comunicații electronice accesibile publicului prin intermediul rețelelor *private* de comunicații.

66. Cu toate acestea, AEPD recunoaște că această formulare ar putea conduce la consecințe neprevăzute și posibil neintenționate. Într-adevăr, simpla trimitere la rețelele private

([15]) „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]) Din contră, s-ar putea spune că deoarece serviciile de comunicații sunt furnizate publicului, chiar dacă rețeaua este privată, furnizarea unor astfel de servicii este reglementată de cadrul juridic existent, în ciuda faptului că rețeaua este privată. De fapt, de exemplu, în Franța, angajatorii care furnizează angajaților acces la internet au fost considerați a fi echivalenți furnizorilor de acces la internet care oferă acces la internet pe baze comerciale. Această interpretare nu este acceptată de toată lumea.

ar putea fi interpretată că reglementează situații pentru care în mod clar nu sunt există intenția de a fi reglementate de directivă. De exemplu, s-ar putea susține că interpretarea literală sau strictă a acestei formulări ar putea aduce în domeniul de aplicare al directivei deținătorii de echipamente WiFi în locuințele acestora ([17]), ceea ce ar da oricui din raza lor de acțiune (de obicei locuința) posibilitatea să se conecteze, deși nu aceasta este intenția amendamentului 121. Pentru a evita acest rezultat, AEPD sugerează reformularea amendamentului 121 astfel încât să se includă în domeniul de aplicare al Directivei privind confidențialitatea în mediul electronic „*prelucrarea de date personale legate de furnizarea de servicii de comunicații electronice accesibile publicului prin intermediul rețelelor publice sau al rețelelor private accesibile publicului din cadrul Comunității, …*”.

67. Aceasta ar ajuta să se clarifice că numai rețelele private care sunt accesibile publicului ar fi reglementate în temeiul Directivei privind confidențialitatea în mediul electronic. Prin aplicarea dispozițiilor Directivei privind confidențialitatea în mediul electronic *numai* rețelelor private accesibile publicului (și nu tuturor rețelelor private), se stabilește o limită, astfel încât directiva va reglementa numai serviciile de comunicații furnizate în rețele private care sunt intenționat menite a fi *accesibile* publicului. Această formulare va ajuta să se sublinieze și mai mult faptul că *disponibilitatea* unei rețele private *publicului larg* este factorul-cheie în a determina dacă directiva ar fi aplicabilă (în afara furnizării unui serviciu de comunicații accesibile publicului). Cu alte cuvinte, independent de faptul că o rețea este publică sau privată, dacă rețeaua a fost intenționat menită a fi accesibilă publicului pentru a furniza un serviciu public de comunicații, cum ar fi accesul la internet, chiar dacă un astfel de serviciu este complementar altuia (de exemplu cazarea hotelieră), acest tip de serviciu/rețea ar fi reglementat de Directiva privind confidențialitatea în mediul electronic.

68. AEPD constată că abordarea sprijinită anterior, potrivit căreia dispozițiile Directivei privind confidențialitatea în mediul electronic sunt aplicate *rețelelor private accesibile publicului*, este compatibilă cu abordările adoptate în unele state membre, în care autoritățile au considerat acest tip de servicii, precum și serviciile furnizate în rețele complet private ca intrând sub incidența dispozițiilor naționale de punere în aplicare a Directivei privind confidențialitatea în mediul electronic ([18]).

69. Pentru a consolida certitudinea juridică cu privire la entitățile reglementate de noul domeniu de aplicare, ar putea fi utilă introducerea în Directiva privind confidențialitatea în mediul electronic a unui amendament care să definească „rețelele private accesibile publicului” după cum urmează: „*rețea privată accesibilă publicului înseamnă o rețea care funcționează într-un spațiu privat ai cărei membri din rândul publicului larg au, de obicei, acces nerestricționat, fie că este sau nu furnizat cu plată sau în completarea unor alte servicii sau oferte, cu condiția acceptării termenilor și condițiilor aplicabile.*”

70. În practică, abordarea sus-menționată ar însemna că sunt reglementate rețele private din hoteluri și alte instituții care furnizează acces la internet publicului larg prin intermediul unei rețele private. Din contră, nu ar fi reglementată furnizarea de servicii de comunicații în rețele complet private, unde serviciul este limitat la un grup restrâns de persoane identificabile. Prin urmare, rețele private virtuale și locuințele consumatorilor echipate cu Wi-Fi nu ar fi reglementate de directivă. Nici serviciile furnizate prin rețele în întregime corporatiste nu ar fi reglementate.

Rețele private care intră sub incidența domeniului de aplicare al Directivei privind confidențialitatea în mediul electronic

71. Excluderea rețelelor private *per se*, așa cum s-a sugerat anterior, ar trebui considerată ca o măsură provizorie care ar trebui să facă obiectul unei dezbateri ulterioare. Într-adevăr, date fiind, pe de o parte, implicațiile privind confidențialitatea ale excluderii rețelelor complet private, și, pe altă parte, faptul că aceasta afectează un mare număr de persoane care de obicei accesează internetul prin intermediul rețelelor corporatiste, este posibil ca pe viitor această excludere să fie reanalizată. Din acest motiv, și pentru a înlesni dezbaterea pe marginea acestui subiect, AEPD recomandă includerea în Directiva privind confidențialitatea în mediul electronic a unui considerent în temeiul căruia Comisia să efectueze o consultare publică privind aplicarea Directivei privind confidențialitatea în mediul electronic la toate rețelele private, cu contribuția AEPD, a autorităților de protecție a datelor și a altor părți interesate relevante. În plus, acest considerent ar putea specifica că, ca rezultat al consultării publice, Comisia ar trebui să facă orice propunere adecvată pentru extinderea sau limitarea tipurilor de entități care ar trebui reglementate de Directiva privind confidențialitatea în mediul electronic.

72. În plus față de cele sus-menționate, diferitele articole ale Directivei privind confidențialitatea în mediul electronic ar trebui modificate astfel încât toate dispozițiile operaționale să facă referire în mod explicit la rețelele private accesibile publicului, pe lângă rețelele publice.

IV. **PRELUCRAREA DATELOR DE TRAFIC ÎN SCOPUL ASIGURĂRII SECURITĂȚII**

73. În cursul procesului legislativ conex revizuirii Directivei privind confidențialitatea în mediul electronic, societățile furnizoare de servicii de securitate au susținut că este necesară introducerea în Directiva privind confidențialitatea în mediul electronic a unei dispoziții care să aducă în legitimitate colectarea datelor de trafic pentru a garanta o securitate online eficientă.

([17]) De obicei rețele locale fără fir (LANs).
([18]) A se vedea nota de subsol nr. 16.

74. Prin urmare, PE a inserat amendamentul 181, care a creat noul articol 6 alineatul (6) litera (a), care ar autoriza în mod explicit prelucrarea datelor de trafic în scopuri de securitate: „Fără a aduce atingere respectării dispozițiilor relevante, altele decât cele prevăzute la articolul 7 din Directiva 95/46/CE și la articolul 5 din prezenta directivă, datele de trafic pot fi prelucrate în interesul legitim al controlorului de date în scopul punerii în aplicare a măsurilor tehnice pentru a garanta securitatea rețelelor informatice și a datelor în sensul articolului 4 litera (c) din Regulamentul (CE) nr. 460/2004 al Parlamentului European și al Consiliului din 10 martie 2004 privind instituirea Agenției Europene pentru Securitatea Rețelelor Informatice și a Datelor, în interesul legitim al unui serviciu public de comunicații electronice, al unei rețele publice sau private de comunicații electronice, al unui serviciu al societății informaționale sau al unui echipament conex terminal sau de comunicație electronică, cu condiția ca acest interes să nu prejudicieze interesul asociat drepturilor și libertăților fundamentale ale persoanei vizate. Prelucrarea datelor trebuie limitată la strictul necesar realizării acestui tip de activități de securitate".

75. Propunerea modificată a Comisiei a acceptat, în principiu, acest amendament, dar prin eliminarea clauzei cu formularea „*Fără a aduce atingere […]… din prezenta directivă*", aceasta a eliminat o clauză-cheie menită să asigure că celelalte dispoziții ale directivei trebuie respectate. Consiliul a adoptat o versiune reformulată, care a făcut încă un pas în direcția diminuării protecțiilor importante și a echilibrării intereselor care erau înscrise în amendamentul 181, prin adoptarea formulării următoare: „*Datele de transfer pot fi prelucrate în măsura strict necesară asigurării securității rețelei și a informațiilor, în conformitate cu articolul 4 litera (c) din Regulamentul (CE) nr. 460/2004 al Parlamentului European și al Consiliului din 10 martie 2004 de înființare a Agenției Europene pentru Securitatea Rețelelor Informatice și a Datelor.*"

76. Astfel cum se descrie mai jos, articolul 6 alineatul (6) litera (a) nu este necesar și este expus riscului de abuz, îndeosebi dacă este adoptat într-o formă care nu include garanțiile importante, clauzele care respectă alte dispoziții ale directivei și echilibrarea intereselor. Prin urmare, AEPD recomandă ca acest articol să fie respins, sau cel puțin, să se asigure faptul că orice articol privind această chestiune include tipurile de garanții care erau incluse în amendamentul 181, astfel cum a fost adoptat de PE.

Fundamente juridice pentru prelucrarea datelor de trafic aplicabile serviciilor de comunicații electronice și altor controlori de date din cadrul legislației actuale privind protecția datelor

77. Măsura în care furnizorii de servicii de comunicații electronice accesibile publicului pot prelucra legal date de trafic este reglementată în temeiul articolului 6 din Directiva privind confidențialitatea în mediul electronic, care restricționează prelucrarea datelor de trafic la un număr de scopuri cum ar fi facturarea, interconectarea și marketingul. Această prelucrare poate avea loc numai în anumite condiții specifice, cum ar fi consimțământul persoanelor în cazul marketingului. În plus, alți controlori de date, cum ar fi furnizorii de servicii ale societății informaționale pot prelucra datele de trafic în temeiul articolul 7 din Directiva privind protecția datelor, care stabilește că controlorii de date pot prelucra date cu caracter personal dacă respectă cel puțin unul dintr-un număr de temeiuri juridice, denumite, de asemenea, fundamente juridice.

78. Un exemplu de astfel de temei juridic este articolul 7 litera (a) din Directiva privind protecția datelor, care impune consimțământul persoanei vizate. De exemplu, dacă un detailist online dorește să prelucreze date de trafic în scopul expedierii de material publicitar sau de marketing, acesta trebuie să obțină consimțământul persoanei. Un alt temei juridic prevăzut în articolul 7 poate permite, în anumite situații, prelucrarea datelor de trafic în scopuri de securitate de către, de exemplu, societățile de securitate care oferă servicii de securitate. Aceasta se bazează pe articolul 7 litera (f) care stabilește că controlorii de date pot prelucra date cu caracter personal dacă „*prelucrarea este necesară pentru realizarea interesului legitim urmărit de operator sau de către unul sau mai mulți terți, cu condiția ca acest interes să nu prejudicieze interesul sau drepturile și libertățile fundamentale ale persoanei vizate…*". Directiva privind protecția datelor nu precizează situațiile în care prelucrarea datelor cu caracter personal ar îndeplini această obligație. Într-adevăr, evaluările sunt efectuate de controlorii de date, de la caz la caz, deseori cu acordul autorităților naționale de protecție a datelor și al altor autorități.

79. Ar trebui luată în considerare coroborarea articolului 7 din Directiva privind protecția datelor cu articolul 6 alineatul (6) litera (a) din Directiva privind confidențialitatea în mediul electronic. Articolul 6 alineatul (6) litera (a) propus este o specificare a situațiilor în care sunt îndeplinite obligațiile menționate la articolul 7 litera (f) prezentate anterior. Într-adevăr, prin autorizarea prelucrărilor datelor de trafic pentru a sprijini asigurarea securității rețelelor și informațiilor, articolul 6 alineatul (6) litera (a) permite prelucrarea în scopurile interesului legitim urmărite de controlorul de date.

80. Astfel cum se descrie mai jos, AEPD consideră că articolul 6 alineatul (6) litera (a) propus nu este nici necesar, nici util. Într-adevăr, din punct de vedere juridic, în principiu, nu este necesar să se stabilească dacă un anumit tip de activitate de prelucrare a datelor, în cazul acesta prelucrarea datelor de trafic în scopuri de securitate, îndeplinește sau nu obligațiile prevăzute la articolul 7 litera (f) din Directiva privind protecția datelor, caz în care consimțământul persoanei poate fi necesar *ex* articolul 7 litera (a). După cum s-a constatat anterior, această evaluare este, de obicei, efectuată de controlorii de date, adică de societăți, la nivelul implementării, în consultare cu autoritățile de protecție a datelor și, dacă este necesar, de către instanță. În general, AEPD consideră că, în anumite cazuri, prelucrarea legitimă a datelor de trafic în scopuri de securitate, efectuată fără a pune în pericol drepturile și libertățile

fundamentale ale persoanelor, este posibil să îndeplinească obligațiile de la articolul 7 litera (f) din Directiva privind protecția datelor și, prin urmare, poate fi efectuată. În plus, nu există niciun alt precedent în Directiva privind protecția datelor și nici în Directiva privind confidențialitatea în mediul electronic care să evidențieze sau să ofere tratament special pentru anumite tipuri de activități de prelucrare a datelor care ar satisface obligațiile de la articolul 7 litera (f), și nici nu s-a demonstrat nevoia unei astfel de excepții. Din contră, după cum s-a constatat mai sus, se pare că în multe situații, acest tip de activități și-ar găsi în mod confortabil locul în textul actual. Prin urmare, o dispoziție juridică care să confirme această evaluare nu este, în principiu, necesară.

Articolul 6 alineatul (6) litera (a) în versiunile Parlamentului European, Consiliului și Comisiei

81. Conform celor expuse anterior, deși inutil, este important să subliniem că amendamentul 181, în forma adoptată de PE, a fost formulat, cu toate acestea, într-o oarecare măsură, ținând seama de principiile confidențialității și protecției datelor prevăzute de legislația privind protecția datelor. Amendamentul 181 al PE ar putea să abordeze în continuare interesele privind protecția datelor și confidențialitatea, de exemplu prin inserarea termenilor „în cazuri specifice" pentru a asigura aplicarea selectivă a acestui articol sau prin includerea unei perioade specifice de păstrare.

82. Amendamentul 181 conține unele elemente pozitive. Acesta confirmă că prelucrarea ar trebui să respecte orice alt principiu de protecție a datelor aplicabil prelucrării datelor cu caracter personal („*Fără a aduce atingere respectării dispozițiilor […] Directivei 95/46/CE și […] din prezenta directivă*"). În plus, deși amendamentul 181 permite prelucrarea datelor de trafic în scopuri de securitate, acesta echilibrează interesele entității care prelucrează datele de trafic cu cele ale persoanelor ale căror date sunt prelucrate astfel încât prelucrările de date să se efectueze numai dacă interesele pentru drepturile și libertățile fundamentale ale persoanelor nu sunt prejudiciate de interesele entității care prelucrează datele („*cu condiția ca acest interes să nu prejudicieze interesul asociat drepturilor și libertăților fundamentale ale persoanei vizate*"). Această obligație este esențială în măsura în care aceasta poate permite prelucrarea de date de trafic pentru cazuri specifice; cu toate acestea, aceasta nu ar permite entității să prelucreze marea masă a datelor de trafic.

83. Versiunea amendamentului reformulat de Consiliu conține elemente lăudabile, cum ar fi menținerea termenului „*strictul necesar*", care subliniază domeniul limitat de aplicare al acestui articol. Cu toate acestea, versiunea Consiliului elimină garanțiile privind protecția datelor și confidențialitatea menționate anterior. În timp ce, în principiu, dispozițiile privind protecția datelor sunt aplicabile, indiferent dacă se face referire specifică în fiecare caz, versiunea articolului 6 alineatul (6) litera (a) a Consiliului poate, cu toate acestea, să fie interpretată că acordă competențe discreționare depline prelucrării datelor de trafic fără a mai face obiectul altor garanții privind protecția datelor și confidențialitatea aplicabile ori de câte ori se prelucrează date. Prin urmare, s-ar putea argumenta că datele de trafic pot fi colectate, stocate sau utilizate în continuare fără a mai trebui să se respecte principiile de protecție a datelor și obligațiile specifice care altfel se aplică părților responsabile, cum ar fi principiul calității sau obligația unei prelucrări echitabile și legale, și de a păstra datele în condiții de confidențialitate și securitate. În plus, deoarece în cadrul articolului nu se face nicio referire la principiile aplicabile privind protecția datelor care impun termene pentru stocarea informațiilor sau la termene specifice, versiunea Consiliului poate fi interpretată că dă posibilitatea colectării și prelucrării datelor de trafic în scopuri de securitate pentru o perioadă de timp neprecizată.

84. În plus, Consiliul a diminuat protecția confidențialității în anumite porțiuni ale textului prin folosirea unor formulări cu sens mai general. De exemplu, referirea la „*interesul legitim al controlorului de date*" a fost eliminată, provocând îndoieli cu privire la tipurile de entități care s-ar putea folosi de această excepție. Este deosebit de important să se evite posibilitatea ca utilizatorii sau entitățile juridice să profite de acest amendament.

85. Experiențele recente ale PE și ale Consiliului demonstrează că este dificil să se definească prin lege măsura și condițiile în care prelucrarea datelor de trafic în scopuri de securitate poate fi executată legal. Este puțin probabil ca orice articol existent sau viitor să îndepărteze riscurile evidente ale unei aplicări prea ample ale excepției din alte motive decât cele legate strict de securitate sau de către entități care ar trebui să nu poată beneficia de această excepție. Aceasta nu înseamnă că o astfel de prelucrare nu se poate efectua în nicio situație. Cu toate acestea, dacă și în ce măsură aceasta poate fi efectuată, se poate mai bine evalua la nivel de implementare. Entitățile care doresc să efectueze astfel de prelucrări ar trebui să discute domeniul și condițiile de aplicare cu autoritățile de protecție a datelor și, eventual, cu Grupul de lucru „articolul 29". Alternativ, Directiva privind confidențialitatea în mediul electronic ar putea include un articol care să permită prelucrarea datelor de trafic în scopuri de securitate, cu condiția unei autorizări explicite acordate de către autoritățile de protecție a datelor.

86. Ținând seama, pe de o parte, de riscurile pe care articolul 6 alineatul (6) litera (a) le creează pentru dreptul fundamental la protecția datelor și la confidențialitate al persoanelor, și, pe de altă parte, de faptul că, astfel cum s-a explicat în prezentul aviz, acest articol nu este necesar, AEPD a ajuns la concluzia că cel mai bun rezultat ar fi ca articolul 6 alineatul (6) litera (a) propus să fie eliminat în întregime.

87. Dacă se adoptă orice text asemănător versiunii actuale a articolului 6 alineatul (6) litera (a), contrar recomandării AEPD, acesta ar trebui, în orice caz, să includă garanțiile privind protecția datelor discutate anterior. Acesta ar trebui, de asemenea, să fie integrat în cadrul structurii existente a articolului 6, de preferat ca un nou alineat (2a).

V. **POSIBILITATEA PERSOANELOR JURIDICE DE A INTENTA ACȚIUNE ÎN JUSTIȚIE ÎN CAZUL ÎNCĂLCĂRII ORICĂREI DISPOZIȚII A DIRECTIVEI PRIVIND CONFIDENȚIALITATEA ÎN MEDIUL ELECTRONIC**

88. PE a adoptat amendamentul 133 care dă posibilitatea furnizorilor de acces la internet și altor entități juridice, cum ar fi asociațiile de consumatori, de a intenta o acțiune în justiție în cazul încălcării oricărei dispoziții a Directivei privind confidențialitatea în mediul electronic ([19]). Din păcate, nici Comisia, nici Consiliul nu l-au acceptat. AEPD consideră acest amendament pozitiv și recomandă menținerea acestuia.

89. Pentru a înțelege importanța acestui amendament, este necesar să se țină seama de faptul că, în domeniul confidențialității și protecției datelor, prejudiciile în sine cauzate unei persoane, în mod individual, nu sunt în general suficiente pentru ca persoana respectivă să intenteze acțiune în justiție. În mod normal, persoanele nu se adresează justiției în mod individual pentru că au fost afectate de spam sau pentru că numele lor a fost în mod eronat inclus într-un director. Acest amendament ar permite asociațiilor de consumatori și sindicatelor care reprezintă interesele consumatorilor la nivel colectiv să deschidă acțiune în justiție în numele acestora. O mai mare diversitate a mecanismelor de aplicare a legii ar putea să încurajeze, de asemenea, un nivel mai bun al respectării legii și, prin urmare, ar fi în interesul unei aplicări eficiente a dispozițiilor Directivei privind confidențialitatea în mediul electronic.

90. În cadrul juridic al unor state membre există precedente juridice care deja prevăd posibilitatea reparațiilor colective pentru a permite consumatorilor și grupurilor de interese să ceară despăgubiri părții care a cauzat prejudiciul.

91. În plus, dreptul concurenței din unele state membre ([20]) dă dreptul consumatorilor, grupurilor de interese (în afara *concurentului afectat*) să deschidă acțiune în justiție împotriva entității vinovată de încălcare. Motivația acestei abordări este că societățile care încalcă dreptul concurenței ar putea să profite, de vreme ce consumatorii cărora li se aduc doar prejudicii marginale se dovedesc, de regulă, reticenți în ceea ce privește intentarea unei acțiuni în justiție. Această motivație poate fi aplicată *mutantis mutandi* în domeniul protecției datelor și al confidențialității.

92. Mai important, astfel cum s-a menționat anterior, acordarea posibilității de a deschidă acțiune în justiție entităților juridice, cum ar fi asociațiile de consumatori și FSCEP, sprijină poziția consumatorilor și respectarea generală a legislației din domeniul protecției datelor. Dacă companiile care se fac vinovate de o încălcare sunt confruntate cu un risc mai mare de a fi date în judecată, este posibil ca acestea să investească mai mult pentru a respecta legislația din domeniul protecției datelor, ceea ce, pe termen lung, va spori nivelul de confidențialitate și de protecție al consumatorilor. Din toate aceste motive, AEPD face apel la Parlamentul European și la Consiliu să adopte o dispoziție care să dea dreptul entităților juridice să intenteze acțiune în justiție pentru în cazul încălcării oricărei dispoziții a Directivei privind confidențialitatea în mediul electronic.

([19]) Articolul 13 alineatul (6) din prima lectură a PE.

([20]) A se vedea, de exemplu, paragraful 8 UWG – Dreptul german privind competiția neloială.

VI. **CONCLUZII**

93. Poziția comună a Consiliului, prima lectură a PE și propunerea modificată a Comisiei conțin, în grade diferite, elemente pozitive care ar fi utile pentru consolidarea protecției confidențialității persoanelor și a datelor personale.

94. Cu toate acestea, AEPD consideră că se mai pot aduce îmbunătățiri, în special cu privire la poziția comună a Consiliului, care, din păcate, nu a menținut unele din amendamentele PE menite să sprijine asigurarea unei protecții adecvate a confidențialității persoanelor și a datelor personale. AEPD îndeamnă PE și Consiliul să refacă garanțiile privind confidențialitatea înscrise în prima lectură a PE.

95. În plus, AEPD consideră că ar fi adecvată simplificarea unora dintre dispozițiile directivei. Acest lucru este adevărat în special în cazul dispozițiilor privind încălcările securității, deoarece AEPD consideră că se vor obține cel mai bine avantaje depline din notificarea încălcărilor dacă cadrul legal este corect stabilit de la bun început. În cele din urmă, AEPD consideră că ar fi adecvate îmbunătățirea și clarificarea formulării unora dintre dispozițiile directivei.

96. Pe baza celor sus-menționate, AEPD îndeamnă PE și Consiliul să-și intensifice eforturile de îmbunătățire și clarificare a unora dintre dispozițiile Directivei privind confidențialitatea în mediul electronic, și să reintroducă, în același timp, amendamentele adoptate în primă lectură de PE, menite să asigure un nivel adecvat de confidențialitate și protecție a datelor. În acest scop, punctele 97, 98, 99 și 100 prezentate în continuare fac rezumatul aspectelor de interes și fac unele recomandări și propuneri de formulare. AEPD face apel la toate părțile implicate să țină seama de acestea în procesul de adoptare finală a Directivei privind confidențialitatea în mediul electronic.

Încălcarea securității

97. Parlamentul European, Comisia și Consiliul au adoptat fiecare diferite abordări pentru notificarea încălcărilor securității. Diferențele între cele trei modele există, printre altele, cu privire la entitățile care intră sub incidența obligației, la standardul sau elementul declanșator al notificării, la persoanele vizate care au dreptul să fie notificate etc. Este necesar ca PE și Consiliul să facă tot ce este posibil pentru a stabili un cadru juridic solid pentru încălcările securității. În acest scop, PE și Consiliul ar trebui:

— să mențină definiția încălcării securității în textele PE, Consiliului și Comisiei, deoarece aceasta este suficient de amplă încât să cuprindă majoritatea situațiilor relevante în care notificarea încălcărilor securității ar putea fi justificată;

— cu privire la domeniul de aplicare al entităților care urmează să intre sub incidența obligației de notificare propuse, *să includă* furnizorii de servicii ai societății informaționale. comercianții cu amănuntul online, băncile online, farmaciile online sunt la fel de expuși riscului de a suferi încălcări ale securității ca și companiile de telecomunicații, dacă nu chiar în măsură și mai mare. Cetățenii se vor aștepta să fie notificați nu numai atunci când furnizorii de acces la internet suferă încălcări ale securității, ci și, în special atunci când aceasta se întâmplă băncilor și farmaciilor online;

— cu privire la elementul declanșator al notificării, standardul propunerii modificate, și anume „*este destul de probabil să aducă prejudicii*", este un standard adecvat care asigură funcționalitatea sistemului. Cu toate acestea, este important să se asigure faptul că „prejudicii" este un termen suficient de amplu încât să cuprindă toate situațiile de efecte negative asupra confidențialității sau asupra altor interese legitime ale persoanelor. În caz contrar, ar fi de preferat să se creeze un nou standard potrivit căruia notificarea să fie obligatorie: „*este destul de probabil ca violarea să aibă efecte nefavorabile asupra persoanelor*". Abordarea Consiliului, care impune ca încălcarea să aducă *grav* atingere confidențialității cuiva, ar asigura protecție inadecvată persoanelor în măsura în care un astfel de standard impune ca efectul asupra confidențialității să fie „grav". Aceasta lasă loc, de asemenea, unei evaluări subiective;

— în timp ce implicarea unei autorități care să stabilească dacă o entitate vizată trebuie să notifice persoane are, desigur, efecte pozitive, este posibil ca aceasta să fie imposibilă în practică sau greu de aplicat și s-ar putea să preia resurse de la alte priorități importante. dacă autoritățile nu pot reacționa extrem de repede, AEPD își manifestă teama că un astfel de sistem poate chiar să diminueze protecția persoanelor și să exercite o presiune nejustificată asupra autorităților. astfel, în general, AEPD recomandă *instituirea unui* sistem prin careevaluarea necesității de notificare să rămână la latitudinea entităților vizate;

— pentru a permite autorităților să-și exercite rolul de supraveghere cu privire la evaluările efectuate de entitățile reglementate privind necesitatea notificării, *să implementeze* următoarele garanții:

  — *să se asigure* că astfel de entități sunt obligate să notifice autoritățile cu privire la orice încălcare care îndeplinește standardul impus;

  — *să confere* autorităților un rol de supraveghere care să le permită să fie selective pentru a putea fi eficiente. pentru a obține cele sus-menționate, să insereze următoarea formulare: „*Dacă abonatul sau persoana vizată nu a fost deja notificată, autoritatea națională competentă, în urma analizării naturii încălcării, poate solicita FSCEP sau FSSI să efectueze notificarea*";

  — *să adopte* o nouă dispoziție care să impună entităților înregistrarea unui parcurs de audit intern detaliat și cuprinzător Aceasta s-ar putea realiza prin adoptarea unei formulări de tipul următor: „*FSCEP și FSSI țin și actualizează o evidență cuprinzătoare care să prezinte în detaliu toate încălcările care au avut loc, informațiile tehnice relevante conexe și măsurile de remediere adoptate. Evidența face, de asemenea, referire la toate notificările emise abonaților sau persoanelor vizate și autorităților naționale competente, inclusiv data și conținutul acestora. Evidența este prezentată autorității naționale competente la cererea acesteia*";

— pentru a asigura coerență în implementarea cadrului încălcărilor securității, *să asigure* Comisiei posibilitatea de a adopta măsuri tehnice de punere în aplicare în urma consultării cu AEPD, Grupul de lucru „articolul 29" și cu alte părți interesate relevante;

— în ceea ce privește persoanele care urmează să fie notificate, *să utilizeze* terminologia Comisiei sau a PE, și anume „persoane vizate" sau „utilizatori afectați", deoarece aceasta include toate persoanele ale căror date cu caracter personal au fost compromise.

Rețelele private accesibile publicului

98. Serviciile de comunicații sunt deseori puse la dispoziția publicului nu prin intermediul rețelelor publice, ci prin rețele care funcționează într-un spațiu privat (de exemplu spațiile Wi-Fi disponibile în hoteluri, aeroporturi), despre care se poate spune că nu sunt reglementate de directivă. PE a adoptat amendamentul 121 (articolul 3) care extinde domeniul de aplicare al directivei pentru a include rețelele publice și private de comunicații electronice, precum și rețelele private accesibile publicului. În această privință, PE și Consiliul ar trebui:

  — *să mențină* elementele principale ale amendamentului 121, dar să-l *reformuleze* astfel încât să includă în domeniul de aplicare al Directivei privind confidențialitatea în mediul electronic numai „*prelucrarea de date personale legate de furnizarea de servicii de comunicații electronice accesibile publicului prin intermediul rețelelor publice sau al rețelelor private accesibile publicului din cadrul Comunității*". rețelele care funcționează exclusiv într-un spațiu privat (spre deosebire de rețelele private accesibile publicului) nu ar fi în mod explicit reglementate;

— *să modifice* în consecință toate dispozițiile operaționale astfel încât să facă referire în mod explicit la rețelele private accesibile publicului, pe lângă rețelele publice;

— *să includă* un amendament care definește: „*rețea privată accesibilă publicului înseamnă o rețea care funcționează într-un spațiu privat ai cărei membri din rândul publicului larg au, de obicei, acces nerestricționat, fie că este sau nu furnizat cu plată sau în completarea unor alte servicii sau oferte, cu condiția acceptării termenilor și condițiilor aplicabile*". Aceasta va sigura o certitudine juridică sporită cu privire la entitățile care intră sub incidența noului domeniu de aplicare;

— *să adopte* un nou considerent pe baza căruia Comisia să efectueze o consultare publică privind aplicarea Directivei privind confidențialitatea în mediul electronic la toate rețelele private, cu contribuția AEPD, a Grupului de lucru „articolul 29" și a altor părți interesate relevante. să specifice că, ca rezultat al consultării publice, Comisia ar trebui să facă orice propunere adecvată pentru extinderea sau limitarea tipurilor de entități care ar trebui reglementate de Directiva privind confidențialitatea în mediul electronic.

Prelucrarea datelor de trafic în scopuri de securitate

99. PE a adoptat în primă lectură amendamentul 181 [articolul 6 alineatul (6) litera (a)], care autorizează prelucrarea datelor de trafic în scopuri de securitate. Poziția comună a Consiliului a adoptat o nouă versiune care diminuează unele din garanțiile privind confidențialitatea. În această privință, AEPD recomandă PE și Consiliului:

— *să respingă* acest articol în întregime deoarece nu este necesar și, dacă este utilizat în mod abuziv, ar putea amenința în mod nejustificat protecția datelor și confidențialitatea persoanelor;

— în mod alternativ, dacă o variantă a versiunii actuale a articolului 6 alineatul (6) litera (a) urmează să fie adoptată, aceasta *să cuprindă* garanțiile de protecție a datelor discutate în prezentul aviz (asemănătoare celor din amendamentul PE).

Acțiunile în justiție pentru încălcări ale Directivei privind confidențialitatea în mediul electronic

100. Parlamentul a adoptat amendamentul 133 [articolul 13 alineatul (6)] care dă posibilitatea entităților să intenteze o acțiune în justiție în cazul încălcării oricărei dispoziții a directivei. Din păcate, Consiliul nu a păstrat acest amendament. Consiliul și PE ar trebui:

— *să adopte* dispoziția care dă dreptul entităților juridice, cum ar fi asociațiile de consumatori și sindicatele, de a intenta o acțiune în justiție în cazul încălcării oricărei dispoziții a directivei (nu numai pentru încălcarea dispozițiilor privind spam-ul, așa cum este actuala abordare a poziției comune și a propunerii modificate). O mai mare diversitate a mecanismelor de aplicare a legii va încuraja un nivel sporit al respectării acesteia și aplicarea eficientă a dispozițiilor Directivei privind confidențialitatea în mediul electronic în întregime.

Soluționarea provocărilor

101. Cu privire la toate chestiunile sus-menționate, PE și Consiliul trebuie să răspundă provocării de a elabora norme și dispoziții care să fie utilizabile și funcționale și, în același timp, să respecte drepturile la confidențialitate și protecția datelor persoanelor. AEPD speră că toate părțile implicate vor face tot posibilul să răspundă acestei provocări și că prezentul aviz va contribui la acest efort.

Adoptat la Bruxelles, 9 ianuarie 2009.

Peter HUSTINX

Autoritatea Europeană pentru Protecția Datelor