I

(Rezoluții, recomandări și avize)

AVIZE

AUTORITATEA EUROPEANĂ PENTRU PROTECȚIA DATELOR

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

(2007/C 255/01)

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 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 [2], și, în special, articolul 41 al acestuia,

ADOPTĂ PREZENTA DECIZIE:

I. INTRODUCERE

1. La 7 martie 2007, 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 [3] a fost transmisă AEPD de către Comisie. În conformitate cu articolul 41 din Regulamentul (CE) nr. 45/2001, AEPD își prezintă avizul.

2. Comunicarea reiterează importanța Directivei 95/46/CE [4] ca punct de reper în istoria protecției datelor cu caracter personal și discută directiva și aplicarea sa în trei capitole: trecutul, prezentul și viitorul. Concluzia principală a comunicării este că directiva nu ar trebui să fie modificată. Punerea în aplicare a directivei ar trebui îmbunătățită prin alte instrumente politice, majoritatea neavând caracter obligatoriu.

3. Avizul AEPD urmărește structura comunicării. Este important de subliniat că AEPD susține concluzia principală a Comisiei potrivită căreia directiva nu ar trebui să fie modificată.

4. Cu toate acestea, AEPD adoptă poziția sus-menționată și din motive pragmatice. Premisele AEPD sunt:

— pe termen scurt, energia ar trebui folosită în vederea îmbunătățirii punerii în aplicare a directivei. Așa cum arată comunicarea, sunt posibile îmbunătățiri considerabile în ceea ce privește punerea sa în aplicare,

— pe termen lung, modificarea directivei nu poate fi evitată, menținându-se totuși principiile esențiale,

— ar trebui să se stabilească deja o dată clară pentru a analiza pregătirea propunerilor de modificare. Această dată reprezintă un stimulent pentru analizarea viitoarelor modificări.

[1] JO L 281, 23.11.1995, p. 31.
[2] JO L 8, 12.1.2001, p. 1.
[3] Denumită în continuare: „comunicarea".
[4] Denumită în continuare: „directiva".

5. Aceste premise sunt esențiale deoarece trebuie luat în considerare faptul că directiva funcționează într-un context dinamic. În primul rând, Uniunea Europeană este în schimbare: circuitul liber de informații între statele membre — și între statele membre și țările terțe — a devenit mai important și va deveni o realitate și mai importantă. În al doilea rând, societatea este în schimbare. Societatea informațională evoluează și preia din ce în ce mai multe caracteristici ale unei societăți de supraveghere ([5]). Acest lucru necesită din ce în ce mai mult protecția eficientă a datelor cu caracter personal pentru a putea face față în mod satisfăcător acestor noi realități.

II. **PERSPECTIVELE AVIZULUI**

6. În vederea evaluării comunicării, AEPD va aborda în special următoarele perspective importante în lumina acestor schimbări:

— îmbunătățirea aplicării directivei: cum poate fi eficientizată protecția datelor? O combinație de instrumente politice este necesară în vederea acestei îmbunătățiri, începând cu o mai bună comunicare cu societatea și continuând cu o mai strictă aplicare a legislației privind protecția datelor,

— interacțiunea cu tehnologia: noi evoluții tehnologice, cum ar fi dezvoltarea programelor de schimb de date, a sistemelor IDFR, a sistemelor de biometrie și de gestionare a identității au un impact clar asupra cerințelor pentru un cadru juridic eficient aplicabil protecției datelor. De asemenea, necesitarea protejării eficiente a datelor cu caracter personal ale persoanelor fizice poate impune limitări privind utilizarea acestor tehnologii noi. Astfel, interacțiunea este dublă: tehnologia influențează legislația iar legislația influențează tehnologia,

— aspecte privind viața privată globală și jurisdicția, care se referă la granițele externe ale Uniunii Europene. Întrucât jurisdicția legiuitorului comunitar este limitată la teritoriul Uniunii Europene, granițele externe sunt mai puțin importante pentru fluxul de date. Economia depinde din ce în ce mai mult de rețelele mondiale. Societățile cu sediul în Uniunea Europeană externalizează din ce în ce mai des activitățile proprii în țări terțe, inclusiv pe cele de prelucrare a datelor cu caracter personal. De asemenea, cazuri recente cum ar fi SWIFT și CNP confirmă că alte jurisdicții își manifestă interesul în „date originare din UE". În general, spațiul fizic în care se realizează operațiunea de prelucrare este mai puțin important,

— protecția datelor și aplicarea legii: amenințări recente la adresa societății, în legătură sau nu cu terorismul, au condus la (cereri pentru) mai multe opțiuni ale organelor de aplicare a legii de a colecta, depozita și schimba datele cu caracter personal. În unele cazuri, părți private iau parte activ la aceste operațiuni, așa cum o demonstrează cazurile recente. Granița care desparte pilonul al treilea din Tratatul privind UE (domeniu în care directiva nu se aplică) devine, pe de o parte, mai importantă și, pe de altă parte, mai fluidă. În unele cazuri, există un risc crescut ca datele cu caracter personal să nu fie protejate de instrumentele specifice primului sau celui de-al treilea pilon („lacuna juridică"),

— consecințele intrării în vigoare a *Tratatului de reformă*, prevăzută în acest moment pentru anul 2009, pentru protecția datelor și aplicarea legii.

III. **TRECUTUL ȘI PREZENTUL**

7. Primul raport privind punerea în aplicare a Directivei privind protecția datelor din 15 mai 2003 cuprindea un program de lucru pentru o mai bună punere în aplicare a Directivei privind protecția datelor, incluzând o listă cu 10 inițiative care urmau să fie realizate între 2003 și 2004. Comunicarea descrie punerea în aplicare a acestor acțiuni.

8. Pe baza analizei activității desfășurate în conformitate cu programul de lucru, comunicarea evaluează pozitiv îmbunătățirile realizate în contextul punerii în aplicare a directivei. Evaluarea Comisiei, rezumată în titlurile capitolului 2 („prezentul") al comunicării, susține în principal următoarele: punerea în aplicare a fost îmbunătățită, deși unele state membre nu au acționat în mod corespunzător; există încă unele divergențe, dar în limitele de manevră prevăzute de directivă și, în orice caz, fără a pune probleme reale pieței interne. Soluțiile juridice prevăzute de directivă s-au dovedit corespunzătoare garantării dreptului fundamental la protecția datelor, ținând cont și de evoluția tehnologiei și de cerințele impuse de interesul public.

9. AEPD susține principalele idei ale acestei evaluări pozitive. În special, AEPD recunoaște efortul considerabil depus în domeniul circuitului transfrontalier de date: concluziile privind protecția corespunzătoare în ceea ce privește țările terțe, noile clauze contractuale standard, adoptarea de reguli corporatiste obligatorii, reflecțiile privind o interpretare mai uniformă a articolului 26 alineatul (1) din directivă și îmbunătățirea procedurilor privind notificările în conformitate cu articolul 26 alineatul (2) au ca scop facilitarea transferurilor internaționale de date cu caracter personal. Cu toate acestea, jurisprudența Curții de Justiție ([6]) a demonstrat că acest domeniu crucial are încă nevoie de modificări pentru a putea face față evoluțiilor în domeniile tehnologiei și aplicării legii.

([5]) A se vedea punctul 37 din prezentul aviz.

([6]) În special sentința Curții în cazurile Lindqvist (a se vedea nota de subsol 15) și CNP (a se vedea nota de subsol 17).

10. În comunicare se mai arată că măsurile de punere în aplicare și de sensibilizare sunt aspecte cheie în promovarea unei mai bune aplicări a directivei și că acestea ar putea fi exploatate în continuare. De asemenea, schimbul celor mai bune practici și armonizarea în domeniul notificărilor și furnizărilor de informații reprezintă precedente de succes pentru înlăturarea birocrației și reducerea costurilor pentru firme.

11. În plus, analiza trecutului confirmă că progresele nu pot fi obținute fără implicarea unui spectru variat de părți interesate. Comisia, autoritățile de protecție a datelor și statele membre sunt jucători importanți în majoritatea acțiunilor întreprinse. Cu toate acestea, rolul părților private are o importanță crescândă, în special când este vorba de promovarea auto-reglementării și a Codurilor Europene de Conduită, sau de dezvoltarea tehnologiilor de consolidare a protecției vieții private.

IV. **VIITORUL**

A. **Concluzia: nicio modificare a directivei în acest moment**

12. Există mai multe motive pentru a susține concluzia Comisiei, potrivit căreia, în circumstanțele de față și pe termen scurt, nicio propunere nu ar trebui avută în vedere pentru modificarea directivei.

13. În esență, Comisia oferă două motive prin care își susține concluzia. În primul rând, potențialul directivei nu a fost utilizat la adevărata sa valoare. Sunt posibile îmbunătățiri considerabile în punerea în aplicare a directivei în jurisdicțiile statelor membre. În al doilea rând, deși directiva lasă loc de manevră statelor membre, nu există nicio dovadă că divergențele în aceste limite ridică probleme reale pieței interne.

14. În baza acestor două motive, Comisia își formulează concluzia astfel: Comisia explică scopul directivei, subliniind rolul acesteia în asigurarea încrederii, și menționează că directiva stabilește un etalon, este neutră din punct de vedere tehnologic și continuă să furnizeze răspunsuri solide și adecvate ([7]).

15. AEPD salută formularea acestei concluzii, dar opinează că aceasta ar putea fi întărită dacă s-ar baza pe două criterii suplimentare:

— în primul rând, natura directivei,

— în al doilea rând, politica legislativă a Uniunii.

Natura Directivei

16. Dreptul fundamental al persoanelor fizice la protecția datelor lor cu caracter personal este recunoscut de articolul 8 din Carta Drepturilor Fundamentale a Uniunii și, *inter alia*, este prevăzut în Convenția Consiliului Europei nr. 108 din 28 ianuarie 1981 pentru protejarea persoanelor față de prelucrarea automatizată a datelor cu caracter personal. În principal, directiva este un cadru care conține principalele elemente ale protecției acestui drept fundamental, atribuindu-i substanță și amplificând drepturile și libertățile incluse în convenție ([8]).

17. Un drept fundamental are ca scop protejarea cetățeanului în toate situațiile, într-o societate democratică. Principalele elemente ale acestui drept fundamental nu ar trebui modificate cu ușurință din cauza evoluțiilor în cadrul societății sau a preferințelor politice ale guvernelor la putere. De exemplu, amenințările organizațiilor teroriste la adresa societății pot conduce la rezultate diferite în cazuri specifice, deoarece sunt necesare interferențe mai importante care să afecteze dreptul fundamental al persoanei, dar nu vor afecta niciodată elementele esențiale ale dreptului în sine și nici nu vor priva sau limita în mod necorespunzător persoanele private de exercitarea acestui drept.

18. A doua caracteristică a directivei este faptul că are în vedere promovarea liberei circulații a informației pe piața internă. De asemenea, acest al doilea obiectiv poate fi considerat fundamental, în cadrul unei piețe interne fără granițe interne în continuă dezvoltare. Armonizarea dispozițiilor esențiale ale legislației naționale este unul din principalele instrumente care asigură înființarea și funcționarea acestei piețe interne. Astfel, se consolidează încrederea reciprocă a statelor membre în sistemele legislative naționale proprii. Modificările ar trebui avute în vedere în mod corespunzător și din aceste motive. Modificările ar putea afecta încrederea reciprocă.

19. O a treia caracteristică a directivei este că trebuie privită ca un cadru general pe care se construiesc instrumente juridice specifice. Aceste instrumente specifice includ măsurile de aplicare a cadrului general, precum și a cadrelor specifice pentru sectoarele corespunzătoare. Directiva 2002/58/CE ([9]) privind viața privată și comunicațiile electronice este un astfel de cadru specific. Acolo unde acest lucru este posibil, evoluțiile în cadrul societății ar trebui să ducă la modificarea măsurilor de aplicare sau a cadrelor juridice specifice și nu la modificarea cadrului general pe care acestea sunt construite.

Politica legislativă a Uniunii

20. În opinia AEPD, concluzia de a nu modifica directiva în acest moment este și consecința logică a principiilor generale de bună administrare și politică legislativă. Propunerile legislative — indiferent dacă se referă la noi domenii de acțiune comunitară sau dacă modifică aranjamentele legislative existente — ar trebui înaintate numai dacă se demonstrează în mod suficient necesitatea și proporționalitatea. Nicio propunere legislativă nu ar trebui înaintată dacă același rezultat ar putea fi obținut utilizând alte instrumente, mai puțin ample.

([7]) Pagina 9, primul paragraf integral al comunicării.

([8]) Considerentul 11 din directivă.

([9]) 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 (Directiva asupra confidențialității și comunicațiilor electronice) (JO L 201, 31.7.2002, p. 37).

21. În situația de față, necesitatea și proporționalitate unei modificări a directivei nu au fost demonstrate. AEPD reamintește faptul că directiva prevede un cadru general pentru protejarea datelor în cadrul dreptului comunitar. Directiva trebuie, pe de o parte, să asigure protecția drepturilor și libertăților persoanelor fizice, în special dreptul acestora la viața privată, în ceea ce privește prelucrarea datelor cu caracter personal și, pe de altă parte, libera circulație a datelor cu caracter personal pe piața internă.

22. Un astfel de cadru general nu ar trebui modificat înainte de a fi pus în aplicare în totalitate în statele membre, decât dacă există indicații clare că obiectivele directivei nu pot fi atinse în cadrul actual. În opinia AEPD, Comisia a fundamentat în mod adecvat — în situația actuală — că directiva nu și-a epuizat potențialul (a se vedea capitolul III din prezentul aviz). De asemenea, nu există nicio dovadă că obiectivele nu ar putea fi atinse în cadrul existent.

B. **Pe termen lung, schimbările par inevitabile**

23. De asemenea, în viitor trebuie ca principiile protecției datelor să ofere o protecție eficientă persoanelor fizice, având în vedere contextul dinamic în care funcționează directiva (a se vedea punctul 5 din prezentul aviz) și perspectivele punctului 6 din prezentul aviz: îmbunătățirea aplicării, interacțiunea cu tehnologia, viața privată globală și jurisdicția, protecția datelor și aplicarea legii, precum și Tratatul de reformă. Nevoia de aplicare completă a principiilor protecției datelor stabilește standardele modificărilor ulterioare care vor afecta directiva. AEPD reamintește că, pe termen lung, modificarea directivei nu poate fi evitată.

24. În ceea ce privește substanța oricăror măsuri ulterioare, AEPD oferă în acest moment unele elemente pe care le consideră esențiale oricărui sistem viitor de protecție a datelor în cadrul Uniunii Europene. Aceste elemente prevăd:

— nu sunt necesare noi principii, dar este clar că sunt necesare alte aranjamente administrative care, pe de o parte, sunt eficiente și adecvate unor societăți interconectate și, pe de altă parte, reduc costurile administrative,

— domeniul de aplicare extins al legislației privind protecția datelor nu ar trebui modificat. Acesta ar trebui să se aplice tuturor utilizărilor de date personale și nu ar trebui să se limiteze la date sensibile, interese calificate sau riscuri speciale. Cu alte cuvinte, AEPD respinge o abordare „*de minimis*” în ceea ce privește obiectul protecției datelor. Astfel, persoanele vizate își vor putea exercita drepturile în toate situațiile,

— legislația privind protecția datelor ar trebuie să acopere, în continuare, o gamă largă de situații dar, în același timp, ar trebui să prevadă o abordare echilibrată în cazuri concrete, luând în considerare alte interese justificate (publice sau private), precum și necesitatea unor consecințe birocratice minime. Acest sistem ar trebui să permită și posibilitatea autorităților de protecție a datelor să stabilească priorități și să se concentreze pe domenii sau aspecte de o importanță deosebită sau care implică riscuri specifice,

— sistemul ar trebui să se aplice în totalitate utilizării datelor personale pentru aplicarea legii, deși ar putea fi necesare măsuri adecvate suplimentare pentru a aborda problemele speciale din acest domeniu,

— ar trebui realizate aranjamente adecvate pentru circulația datelor cu țările terțe, în măsura în care acest lucru este posibil, pe baza standardelor mondiale pentru protecția datelor.

25. Referitor la provocările lansate de noile tehnologii, comunicarea menționează analiza continuă a Directivei 2002/58/CE și posibila necesitate de norme mai specifice care să abordeze aspectele privind protecția datelor pe care le ridică noile tehnologii, cum ar fi internetul și IDFR ([10]). AEPD salută această analiză și acțiunile ulterioare deși, conform AEPD, acestea nu ar trebui să se refere numai la evoluții tehnologice, ci ar trebui să ia în calcul contextul dinamic în întregime și să implice, pe termen lung, și Directiva 95/46/CE. De asemenea, trebuie insistat pe acest aspect. Din păcate, comunicarea are un final deschis:

— nu există nici un termen pentru realizarea diverselor activități menționate la capitolul 3 al comunicării,

— nu există niciun termen pentru un raport ulterior privind aplicarea directivei. Articolul 33 din directivă prevede ca un raport „periodic” să fie emis de Comisie, dar nu specifică intervalele de timp,

— nu există specificații: Comunicarea nu permite evaluarea gradului de realizare a activităților avute în vedere. Se referă doar la programul de lucru prezentat în 2003,

— nu indică modalitățile de acțiune pe termen lung.

AEPD propune ca pe viitor Comisia să specifice aceste elemente.

([10]) Pagina 11 din comunicare.

V. **PERSPECTIVELE SCHIMBĂRII ÎN VIITOR**

A. **Aplicarea integrală**

26. Orice modificare ulterioară trebuie să fie precedată de aplicarea integrală a dispozițiilor actuale ale Directivei. Aplicarea integrală începe cu respectarea cerințelor juridice ale directivei. Comunicarea menționează ([11]) faptul că unele state membre nu au reușit să încorporeze numeroase dispoziții importante ale directivei și subliniază în special dispozițiile privind independența autorităților de supraveghere. Comisia are sarcina de a monitoriza respectarea și, în cazul în care consideră necesar, de a face uz de atribuțiile conferite de articolul 226 CE.

27. Comunicarea are în vedere o interpretare a anumitor dispoziții, în special a celor care ar putea duce la proceduri formale de încălcare, în conformitate cu articolul 226 CE.

28. De asemenea, directiva introduce alte mecanisme pentru îmbunătățirea procesului de punere în aplicare. Sarcinile Grupului de lucru „articolul 29", menționate la articolul 30 din directivă, au fost concepute în acest scop. Acestea au în vedere stimularea aplicării protecției datelor la un nivel ridicat și armonizat în statele membre dincolo de ceea ce este strict necesar pentru îndeplinirea obligațiilor prevăzute de directivă. În vederea exercitării acestui rol, Grupul de lucru a produs, pe parcursul mai multor ani, un număr ridicat de avize și alte documente.

29. În opinia AEPD, aplicarea integrală a directivei include aceste două elemente:

— trebuie să ne asigurăm că statele membre îndeplinesc în întregime obligațiile pe care le au în conformitate cu dreptul european. Aceasta înseamnă că dispozițiile directivei trebuie transpuse în legislația națională și în practică trebuie atinse rezultatele pe care directiva trebuie să le obțină,

— în caz contrar, instrumentele neobligatorii care ar putea fi esențiale pentru obținerea unui nivel ridicat și armonizat de protecție a datelor ar trebui utilizate în totalitate.

AEPD subliniază că ambele elemente trebuie distinse cu claritate, datorită consecințelor juridice diferite, precum și a responsabilităților aferente. Ca regulă generală: Comisia ar trebui să-și asume responsabilitatea deplină pentru primul element, iar Grupul de lucru ar trebui să fie principalul jucător în ceea ce privește al doilea element.

30. O altă distincție mai precisă care trebuie făcută se referă la instrumentele disponibile pentru o mai bună aplicare a directivei. Acestea includ:

— măsurile de punere în aplicare. Aceste măsuri — asumate de Comisie prin procedura de comitologie — sunt prevăzute în capitolul IV, privind transferul datelor cu caracter personal țărilor terțe [a se vedea articolul 25 alineatul (6) și articolul 26 alineatul (3)],

— legislația sectorială,

— procedurile de încălcare prevăzute de articolul 226 CE,

— comunicarea de interpretare. Aceste comunicări ar putea să se concentreze pe dispozițiile care pot duce la aplicarea procedurilor de încălcare și/sau care să fie utilizate numai ca ghid pentru protecția datelor în practică (a se vedea și punctele 57-62) ([12]),

— alte comunicări. Comunicarea Comisiei către Parlamentul European și Consiliu privind tehnologiile de protecție a vieții private poate fi luată ca exemplu,

— promovarea celor mai bune practici. Acest instrument poate fi folosit pentru o serie de subiecte, cum ar fi simplificarea procedurilor administrative, audit, aplicare și sancțiuni etc. (a se vedea și punctele 63-67).

31. AEPD îi propune Comisiei să indice cu claritate modalitățile de utilizare a acestor instrumente diverse în momentul în care va elabora strategiile pe baza prezentei comunicări. În acest context, Comisia ar trebui să distingă cu claritate între propriile responsabilități și cele ale Grupului de lucru. Pe lângă acestea, nu prezintă nicio noutate faptul că o bună cooperare între Comisie și Grupul de lucru este o condiție a succesului.

B. **Interacțiunea cu tehnologia**

32. Se pleacă de la premisa că dispozițiile directivei sunt formulate într-un limbaj tehnologic neutru. Comunicarea leagă importanța acordată neutralității tehnologice de o serie de evoluții tehnologice, cum ar fi internetul, serviciile de acces furnizate în țări terțe, IDFR și o combinație de date sub formă de sunet și imagine cu recunoaștere automată. Aceasta distinge două tipuri de acțiuni. În primul rând, îndrumare specifică în ceea ce privește aplicarea principiilor de protecție a datelor într-un mediu tehnologic în continuă schimbare, un rol important avându-l Grupul de lucru și propriul departament Internet Task Force ([13]). În al doilea rând, Comisia ar putea să propună legislația specifică sectorului.

33. AEPD salută această abordare ca un prim pas important. Cu toate acestea, pe termen lung sunt necesari pași fundamentali. Această comunicare ar putea fi folosită ca preludiul unei abordări pe termen lung. AEPD propune inițierea unei discuții pe această temă, în lumina prezentei comunicări. Următoarele puncte pot fi menționate ca posibile elemente ale unei astfel de abordări.

([11]) Pagina 6 din comunicare, lângă alineatul final.

([12]) A se vedea, de exemplu, Avizul nr. 4/2007 privind conceptul de date cu caracter personal (GL 137) al Grupului de lucru, adoptat la 20 iunie 2007.

([13]) Internet Task Force este un subgrup al Grupului de lucru „articolul 29".

34. În primul rând, interacțiunea cu tehnologiile este dublă: Pe de o parte, noile tehnologii în curs de dezvoltare pot impune modificarea cadrului juridic aplicabil protecției datelor. Pe de altă parte, necesitarea protejării eficiente a datelor cu caracter personal ale persoanelor fizice poate impune limitări noi sau măsuri de protecție adecvate privind utilizarea anumitor tehnologii, o consecință și mai importantă. Cu toate acestea, noile tehnologii ar putea fi utilizate eficient pentru a asigura respectarea vieții private.

35. În al doilea rând, s-ar putea impune unele limitări specifice în cazul în care noile tehnologii vor fi utilizate de instituții guvernamentale în exercitarea atribuțiilor publice ale acestora. Discuțiile privind interoperabilitatea și accesul care au loc în domeniul libertății, securității și justiției privind aplicarea Programului de la Haga sunt un bun exemplu ([14]).

36. În al treilea rând, există tendința utilizării pe scară largă a materialului biometric, cum ar fi materialul ADN, dar nu numai. Provocările specifice ale utilizării datelor cu caracter personal extrase din acest material ar putea avea consecințe asupra legislației privind protecția datelor.

37. În al patrulea rând, trebuie recunoscut faptul că și societatea se schimbă și preia din ce în ce mai multe elemente ale unei societăți de supraveghere ([15]). O dezbatere fundamentală este necesară în această privință. În această dezbatere, întrebările esențiale ar putea fi dacă această evoluție nu poate fi evitată, dacă legiuitorul european are datoria să influențeze evoluția și să impună limite, dacă și cum ar putea legiuitorul european să ia măsuri eficiente etc.

C. **Viața privată globală și jurisdicția**

38. Aspecte privind viața privată globală și jurisdicția joacă un rol limitat în Comunicare. Singura intenție în acest context este continuarea de către Comisie a monitorizării forurilor internaționale și contribuirea la acestea, pentru a asigura coerența dintre angajamentele statelor membre și obligațiile acestora prevăzute în directivă. Pe lângă acestea, comunicarea amintește o serie de activități realizate pentru simplificarea cerințelor pentru transferuri internaționale (a se vedea capitolul III din prezentul aviz).

39. AEPD regretă că acestei perspective nu i-a fost acordat un rol mai important în comunicare.

40. În acest moment, capitolul IV din directivă (articolele 25 și 26) introduce un regim special pentru transferul de date către țările terțe, pe lângă regulile generale privind protecția datelor. Acest regim special a fost elaborat de-a lungul anilor, cu intenția de a realiza un echilibru între protecția persoanelor fizice ale căror date sunt transferate țărilor terțe și, *inter alia*, imperativele comerțului internațional și realitatea rețelelor mondiale de telecomunicații. Comisia și Grupul de lucru ([16]), dar și Camera Internațională de Comerț, de exemplu, au depus un efort considerabil în rentabilizarea acestui sistem, prin analize privind adecvarea nivelului de protecție al datelor, clauze contractuale standard, reguli corporatiste obligatorii etc.

41. Sentința Curții de Justiție în cazul *Lindqvist* ([17]) are o deosebită importanță pentru aplicabilitatea sistemului la internet. Curtea subliniază caracterul ubicuu al informațiilor de pe internet și decide că încărcarea datelor pe o pagină internet ca atare, chiar dacă datele sunt accesibile persoanelor în țări terțe dacă dispun de mijloacele tehnice pentru a le accesa, nu reprezintă transfer către țări terțe.

42. Acest sistem, o consecință logică și necesară a limitărilor teritoriale din Uniunea Europeană, nu va asigura protecția deplină a persoanelor europene vizate într-o societate interconectată în care granițele fizice își pierd din importanță (a se vedea exemplele menționate la punctul 6 din prezentul aviz): informațiile de pe internet sunt ubicue, dar jurisdicția legiuitorului european nu.

43. Provocarea constă în identificarea de soluții practice care să reconcilieze nevoia de protecție a persoanelor vizate europene cu limitările teritoriale ale Uniunii Europene și ale statelor membre. Prin comentariile sale referitoare la Comunicarea Comisiei privind o strategie cu privire la dimensiunea externă a spațiului de libertate, securitate și justiție — AEPD a încurajat Comisia să joace un rol activ în promovare protecției datelor cu caracter personal la nivel internațional, susținând abordări bilaterale și multilaterale cu țări terțe și cooperarea cu alte organizații internaționale ([18]).

([14]) A se vedea, de exemplu, Comentariile la Comunicarea Comisiei privind interoperabilitatea bazelor de date europene, 10 martie 2006, publicate pe site-ul AEPD.

([15]) A se vedea: „Raportul privind societatea de supraveghere", elaborat de Surveillance Studies Network pentru Comisarul britanic pentru informații și prezentat la a 28-a Conferință internațională a comisarilor pentru protecția datelor și viață privată, la Londra, între 2 și 3 noiembrie 2006 [a se vedea: www.privacyconference2006.co.uk (secțiunea Documente)].

([16]) A se vedea, de exemplu, Documentul de lucru privind interpretarea comună a articolului 26 alineatul (1) din Directiva 95/46/CE din 24 octombrie 1995, adoptat la 25 noiembrie 2005 (GL 114); Documentul de lucru privind stabilirea unei proceduri de cooperare pentru emiterea de opinii comune privind garanțiile adecvate ce rezultă din „Regulile Corporatiste Obligatorii", adoptat la 14 aprilie 2005 (GL 107) și Avizul 8/2003 privind proiectul de clauze contractuale standard înaintat de un grup de asociații patronale („modelul alternativ de contract") adoptat la 17 decembrie 2003 (GL 84).

([17]) Sentința Curții din 6 noiembrie 2003, cazul C-101/01, ECR [2003], p. I-12971, punctele 56-71.

([18]) A se vedea Scrisoarea Directorului general al departamentului pentru justiție, libertate și securitate al Comisiei europene asupra Comunicării „O strategie cu privire la dimensiunea externă a spațiului de libertate, securitate și justiție", 28 noiembrie 2005, disponibilă pe site-ul AEPD.

44. Aceste soluții practice includ:

— evoluția ulterioară a unui cadru global pentru protecția datelor; standarde mai larg acceptate, cum ar fi instrucțiunile OCDE pentru protecția datelor (1980) și instrucțiunile Organizației Națiunilor Unite ar putea sta la baza acestora,

— evoluția ulterioară a unui regim special pentru transferul de date către țările terțe, conform capitolului IV din directivă (articolele 25 și 26),

— acorduri internaționale privind jurisdicția sau alte acorduri similare cu țări terțe,

— investiții în mecanisme pentru conformitate globală, cum ar fi utilizarea de reguli corporatiste obligatorii de către societățile multinaționale, indiferent dacă datele cu caracter personal sunt prelucrate de acestea sau nu.

45. Niciuna dintre aceste soluții nu este nouă. Cu toate acestea, se impune o viziune pentru eficientizarea utilizării acestor metode și pentru a asigura respectarea standardelor de protecție a datelor — care, în Uniunea Europeană, reprezintă drepturi fundamentale — cu eficiență, într-o societate globală interconectată. AEPD invită Comisia să inițieze elaborarea unei viziuni în această privință, împreună cu părțile implicate cele mai importante.

D. **Aplicarea legii**

46. Comunicarea acordă o atenție deosebită cererilor impuse de interesul public, în special în ceea ce privește siguranța. Aceasta explică articolul 3 alineatul (2) din directivă și interpretarea dată de Curtea de Justiție cu privire la această dispoziție în sentința CNP ([19]) precum și articolul 13 din directivă, referitor, printre altele, la jurisdicția Curții europene pentru drepturile omului. De asemenea, comunicarea subliniază că, atunci când Comisia atinge un echilibru important între măsurile necesare pentru asigurarea securității și protejarea drepturilor fundamentale care nu sunt negociabile, aceasta se asigură că protejează datele personale conform articolului 8 din CEDO. Acest punct de plecare se aplică și dialogului transatlantic cu Statele Unite ale Americii.

47. Conform AEPD, Comisia trebuie să reitereze cu claritate obligațiile Uniunii în baza articolului 6 din Tratatul privind Uniunea Europeană privind respectarea drepturilor fundamentale, garantate de CEDO. Această declarație este cu atât mai importantă cu cât Consiliul European a decis ca, în conformitate cu *Tratatul de reformă*, Carta Drepturilor Fundamentale a Uniunii Europene să aibă valoare juridică obligatorie. Articolul 8 din Cartă recunoaște dreptul tuturor la protecția datelor cu caracter personal.

48. Se știe că cererile organelor de aplicare a legii de utilizare tot mai frecventă a datelor cu caracter persona pentru combaterea infracționalității — fără să menționăm combaterea terorismului — pot rezulta în diminuarea nivelului de protecție a cetățeanului, sub nivelul garantat de articolul 8 CEDO și/sau de Convenția Consiliului Europei nr. 108 ([20]). Aceste preocupări au reprezentat un element important al celui de-al treilea aviz al AEPD cu privire la Propunerea de decizie-cadru a Consiliului privind protecția datelor cu caracter personal prelucrate în cadrul cooperării dintre poliție și justiție în materie penală, emis la 27 aprilie 2007.

49. În acest context, este esențial ca standardul de protecție prevăzut de directivă să fie preluat ca fundament pentru protecția cetățenilor, în ceea ce privește solicitările de aplicare a legii. CEDO și Convenția nr. 108 prevăd un nivel minim de protecție, dar nu oferă precizia necesară. Pe lângă acestea, au fost necesare măsuri suplimentare pentru asigurarea unei protecții adecvate a cetățeanului. Această necesitate a reprezentat unul dintre factorii esențiali pentru adoptarea directivei ([21]) în 1995.

50. Este la fel de important ca acest standard de protecție să fie garantat cu eficiență în toate situațiile în care datele cu caracter personal sunt prelucrate pentru aplicarea legii. Deși această comunicare nu se referă la prelucrarea datelor în cadrul celui de-al treilea pilon, abordează în mod corect situația în care datele colectate (și prelucrate) în scopuri comerciale sunt utilizate pentru aplicarea legii. O situație care devine uzuală pe măsură ce activitatea poliției depinde din ce în ce mai mult pe disponibilitatea informațiilor deținute de terțe părți. Directiva 2006/24/CE ([22]) poate fi privită ca o bună ilustrare a acestei tendințe: această directivă obligă furnizorii de comunicații electronice să depoziteze (pe o perioadă mai lungă) datele pe care le-au colectat (și depozitat) în scopuri comerciale, în vederea îndeplinirii cerințelor organelor de aplicare a legii. Conform AEPD, trebuie ca datele cu caracter personal colectate și prelucrate în cadrul prevederilor directivei să fie protejate în mod corespunzător atunci când sunt utilizate în interesul public și, în special, în cadrul operațiunilor de securitate sau de luptă împotriva terorismului. Cu toate acestea, în unele cazuri, scopurile recent menționate nu cad sub incidența directivei.

([19]) Sentința Curții din 30 mai 2006, Parlamentul European vs. Consiliul (C-317/04) și Comisia (C-318/04), cazurile conexe 1 C-317/04 și C-318/04, ECR [2006], p. I-4721.

([20]) Convenția Consiliului Europei pentru protejarea persoanelor față de prelucrarea automatizată a datelor cu caracter personal, 28 ianuarie 1981.

([21]) Lipsa de precizie a Convenției nr. 108 a fost menționată de AEPD într-o serie de avize referitoare la necesitatea unei decizii-cadru a Consiliului.

([22]) Directiva 2006/24/CE a Parlamentului European și a Consiliului din 15 martie 2006 privind păstrarea datelor generate sau prelucrate în legătură cu furnizarea serviciilor de comunicații electronice accesibile publicului sau de rețele de comunicații publice și de modificare a Directivei 2002/58/CE (JO L 105, 13.4.2006, p. 54).

51. Aceste observații conduc la următoarele propuneri făcute Comisiei:

— o analiză aprofundată este necesară asupra implicațiilor la adresa protecției datelor în cazul implicării societăților private în activități de aplicare a legii, pentru ca principiile Directivei 95/46/CE să se aplice în totalitate acestor situații și pentru ca nicio lacună să nu afecteze dreptul fundamental al cetățenilor la protecția datelor. În special, trebuie ca datele cu caracter personal colectate în cadrul prevederilor directivei să fie protejate în mod corespunzător și consecvent atunci când sunt prelucrate ulterior în interesul public, fie că sunt sau că nu sunt sub incidența directivei,

— această analiză ar trebui să includă, în orice caz, neajunsurile cadrului juridic actual, deoarece granița dintre primul și cel de-al treilea pilon este neclară și ar putea exista situații în care să nu existe o bază adecvată pentru un instrument juridic pentru protecția datelor ([23]),

— articolul 13 din directivă, care permite restricții și derogări de la principiile protecției datelor, atunci când este necesar, *inter alia*, în interesul public, ar trebui interpretat pentru a menține *efectul util* ca interfață esențială și garanție a datelor cu caracter personal colectate în cadrul dispozițiilor directivei, în conformitate cu sentința Curții de Justiție în cazul *Österreichischer Rundfunk* ([24]) și cu jurisdicția CEDO,

— ar trebui să fie luată în considerare posibilitatea de a se propune o legislație care să aibă ca scop armonizarea condițiilor și garanțiilor de utilizare a derogărilor prevăzute în articolul 13.

E. **Situația posibilă în conformitate cu Tratatul de reformă**

52. În Comunicare, Comisia analizează enormul impact al Tratatului constituțional în ceea ce privește protecția datelor. Într-adevăr, Tratatul — care a devenit Tratat de reformă — va avea o importanță deosebită în acest sector. Tratatul va reprezenta sfârșitul structurii pe piloni, dispozițiile privind protecția datelor (în acest moment articolul 286 CE) vor fi clarificate, iar Carta Drepturilor Fundamentale a Uniunii, care include o dispoziție privind protecția datelor la articolul 8, va deveni instrument obligatoriu.

53. Mandatul conferinței interguvernamentale (CIG) acordă o atenție deosebită protecției datelor. Articolul 19 litera (f) prevede, în principal, trei aspecte. În primul rând, regulile generale privind protecția datelor nu vor aduce atingere normelor specifice adoptate în Titlul PESC (în prezent al doilea pilon); în al doilea rând, se va adopta o declarație privind protecția datelor în domeniul cooperării polițienești și judiciare în materie penală (al treilea pilon) și în al treilea rând, se vor adopta intrări specifice în protocoalele relevante cu privire la poziția statelor membre (acest element se referă în special la poziția diferită a Regatului Unit cu privire la cooperarea polițienească și judiciară în materie penală).

54. Al doilea element (declarația) va trebui clarificat în cadrul CIG. Consecințele anulării structurii pe piloni și posibila aplicare a Directivei privind cooperarea polițienească și judiciară în materie penală vor trebui luate în considerare pentru a asigura o aplicare cât mai extinsă a principiilor de protecție a datelor cuprinse în directivă. Nu vom discuta aici detaliile acestor aspecte. AEPD și-a prezentat propunerile pentru declarație într-o scrisoare adresată președinției CIG ([25]).

VI. **INSTRUMENTE PENTRU O MAI BUNĂ APLICARE**

A. **Generalități**

55. Comunicarea face referire la o serie de instrumente și acțiuni care pot fi utilizate pentru o mai bună aplicare a directivei pe viitor. AEPD dorește să le comenteze, explorând alte instrumente suplimentare, nemenționate în Comunicare.

B. **Legislația sectorială**

56. În anumite cazuri, acțiuni legislative specifice ar putea fi necesare la nivel european. În mod deosebit, legislația sectorială s-ar putea dovedi necesară pentru a adapta principiile directivei la aspectele ridicate de anumite tehnologii, cum este cazul directivelor privind viața privată în sectorul telecomunicațiilor. Utilizarea legislației specifice trebuie analizată cu atenție în domenii cum ar fi utilizarea tehnologiilor IDFR.

C. **Proceduri de încălcare**

57. Procedura de încălcare este cel mai important instrument menționat în comunicare. Comunicarea identifică un domeniu specific care ridică probleme, și anume independența autorităților de protecție a datelor și atribuțiile acestora, și menționează alte domenii doar în termeni generali. AEPD împărtășește opinia potrivit căreia procedurile de încălcare sunt un instrument esențial și inevitabil în cazul în care statele membre nu asigură o aplicare deplină a directivei, în special luând în considerare faptul că au trecut aproape nouă ani de la termenul de punere în aplicare a directivei și că dialogul structurat prevăzut în programul de lucru a avut deja loc. Cu toate acestea, în momentul de față, în fața Curții de Justiție nu a fost prezentat niciun caz de încălcare a Directivei 95/46.

([23]) Aspectul unui „cerc vicios”, exprimat de AEPD în mai multe ocazii, în principal referitor la Sentința CNP (a se vedea, de exemplu, raportul anual 2006, p. 47).

([24]) Sentința Curții din 20 mai 2003, cazurile conexe C-465/00, C-138/01 și C-139/01, ECR [2003] p. I-4989.

([25]) A se vedea scrisoarea AEPD din 23 iulie 2007 adresată președinției CIG cu privire la protecțiadatelor în cadrul Tratatului de reformă, disponibilă pe site-ul AEPD.

58. O analiză comparativă a tuturor cazurilor în care se suspectează o transpunere eronată sau incompletă ([26]), precum și o comunicare de interpretare pot îmbunătăți cu siguranță coerența rolului Comisiei ca gardian al Tratatelor. Cu toate acestea, elaborarea acestor instrumente, care ar putea necesita un anumit timp și efort, nu ar trebui să amâne procedurile de încălcare în acele domenii în care transpunerea sau practica incorectă au fost deja identificate cu claritate de către Comisie.

59. Prin urmare, AEPD încurajează Comisia să urmărească o mai bună punere în aplicarea a directivei, prin proceduri de încălcare, dacă este cazul. În acest context, AEPD va face uz de atribuțiile sale de intervenție pe lângă Curtea de Justiție pentru a interveni, acolo unde este cazul, în procedurile de încălcare referitoare la aplicarea Directivei 95/46 sau la alte instrumente juridice în domeniul protecției datelor cu caracter personal.

D. **Comunicarea de interpretare**

60. Comunicarea se referă și la comunicarea de interpretare a unor dispoziții în care Comisia își va clarifica poziția cu privire la dispozițiile directivei a căror implementare este considerată problematică și care ar putea duce la aplicarea procedurilor de încălcare. AEPD salută faptul că în acest context Comisia va lua în considerare activitatea de interpretare desfășurată de Grupul de lucru. Într-adevăr, este esențial ca poziția Grupului de lucru să fie luată în considerare în mod corespunzător în cadrul elaborării viitoarei comunicări de interpretare și ca Grupul de lucru să fie consultat în mod adecvat, pentru a contribui cu experiența proprie la aplicarea directivei la nivel național.

61. De asemenea, AEPD își confirmă disponibilitatea de a consilia Comisia în toate aspectele referitoare la protecția datelor cu caracter personal. Acest lucru se aplică și acelor instrumente, cum ar fi comunicările Comisiei, care nu au caracter obligatoriu dar care au totuși ca scop definirea politicii Comisiei în domeniul protecției datelor cu caracter personal. În cazul comunicărilor, pentru ca acest rol consultativ să fie eficient, consultarea AEPD ar trebui să aibă loc înainte de adoptarea comunicării de interpretare ([27]). Rolul consultativ al GL 29 și al AEPD va aduce o valoare adăugată la această comunicare, păstrând în același timp independența Comisiei de a decide autonom cu privire la deschiderea oficială a procedurilor de încălcare referitoare la aplicarea directivei.

62. AEPD salută faptul că această comunicare se referă la un număr limitat de articole, concentrându-se astfel pe aspecte mai sensibile. În acest sens, AEPD atrage atenția Comisiei cu privire la următoarele aspecte, care necesită o atenție deosebită în comunicarea de interpretare:

— conceptul de date cu caracter personal ([28]),

— definirea rolului operatorului de date sau a persoanei împuternicite de către operator,

— stabilirea legislației aplicabile,

— principiul limitării obiectivului și utilizarea incompatibilă,

— fundamentele juridice pentru prelucrare, în special în ceea ce privește consimțământul neechivoc și echilibrul între interese.

E. **Alte instrumente neobligatorii**

63. Alte instrumente neobligatorii ar trebui să afecteze în mod activ respectarea principiilor de protecție a datelor, în special în medii în care se utilizează noile tehnologii. Aceste măsuri ar trebui construite pe principiul „viață privată prin concepție" („privacy by design"), asigurând dezvoltarea și construcția arhitecturii noilor tehnologii în conformitate cu principiile protecției datelor. Promovarea produselor tehnologice care respectă viața privată ar trebui să fie un element esențial în contextul în care mediul informatic ubicuu se dezvoltă cu rapiditate.

64. Necesitatea creșterii numărului părților implicate în aplicarea legislației privind protecția datelor este strâns legată de ce s-a menționat anterior. Pe de o parte, AEPD sprijină cu fermitate rolul fundamental al autorităților de protecție a datelor în aplicarea principiilor directivei, utilizând pe deplin atribuțiile de care dispun precum și posibilitățile de coordonare în cadrul Grupului de lucru „articolul 29". Aplicarea mai eficientă a directivei constituie și unul din obiectivele „inițiativei de la Londra".

65. Pe de altă parte, AEPD subliniază necesitatea de a promova aplicarea privată a principiilor protecției datelor prin auto-reglementare și concurență. Agenții economici ar trebui încurajați să aplice principiile de protecție a datelor și să concureze în dezvoltarea de produse și servicii care respectă viața privată ca mijloc de extindere a pozițiilor acestora pe piață printr-o mai bună satisfacere a așteptărilor consumatorilor conștienți de dreptul lor la viața privată. În acest context, un bun exemplu îl reprezintă mărcile de protecție a vieții private, care pot fi atașate produselor sau serviciilor ce au făcut obiectul unei proceduri de certificare ([29]).

([26]) A se vedea Comunicarea, p. 6.

([27]) A se vedea documentul de strategie al AEPD „AEPD — consilier al instituțiilor comunitare pentru propuneri legislative și documente conexe", disponibil pe site-ul AEPD (punctul 5.2 din document).

([28]) Acest aspect a fost abordat și în avizul nr. 4/2007 al Grupului de lucru, citat în nota de subsol 9.

([29]) Merită menționat proiectul EuroPriSe, promovat de Autoritatea pentru protecția datelor din Schleswig Holstein în cadrul proiectului Èten al Comisiei Europene.

66. AEPD dorește, de asemenea, să atragă atenția Comisiei asupra altor instrumente care, deși nu sunt menționate în comunicare, s-ar putea dovedi utile pentru o mai bună aplicare a directivei. Exemple de astfel de instrumente care ar putea ajuta autoritățile de protecție a datelor să aplice mai bine legislația privind protecția datelor sunt:

— analiza comparativă,

— promovarea și partajarea celor mai bune practici,

— audituri ale terților privind viața privată.

F. **Alte instrumente, pe termen lung**

67. Ca un ultim punct, AEPD se referă la alte instrumente care nu sunt menționate în comunicare dar care ar putea fi luate în considerare în cazul modificării directivei sau ar putea fi incluse în legislația orizontală, în special:

— acțiunile colective, care permit unor grupuri de cetățeni să introducă acțiuni comune în materie de protecție a datelor cu caracter personal, ar putea constitui un instrument foarte important de facilitare a aplicării directivei,

— acțiunile introduse de persoane juridice ale căror activități au ca scop protejarea intereselor anumitor categorii de persoane, cum ar fi asociațiile de consumatori și sindicatele, ar putea avea un efect similar,

— obligațiile operatorilor de a notifica persoanelor vizate încălcările procedurilor de securitate ar putea constitui atât un mijloc de protecție util, cât și un mod de a spori gradul de sensibilizare al cetățenilor,

— dispozițiile care facilitează utilizarea de mărci de protecție a vieții private sau auditurile terților (a se vedea punctele 65 și 66) într-un cadru transnațional.

G. **O mai bună definire a responsabilităților actorilor instituționali, în special ale Grupului de lucru**

68. Diverși actori instituționali au responsabilități în ceea ce privește punerea în aplicare a directivei. În conformitate cu articolul 28 din directivă, autoritățile de supraveghere din statele membre sunt responsabile de supravegherea aplicării dispozițiilor naționale care transpun directiva în statele membre. Articolul 29 introduce Grupul de lucru al autorităților de supraveghere iar articolul 30 menționează sarcinile acestuia. În conformitate cu articolul 31, un comitet de reprezentanți ai guvernelor statelor membre sprijină Comisia în legătură cu punerea în aplicare a măsurilor la nivel comunitar (comitet de tipul celor prevăzute în procedurile în materie de comitologie).

69. Nevoia unei mai bune definiri a responsabilităților diferiților actori există în special în legătură cu (activitățile) Grupul(ui) de lucru. Articolul 30 alineatul (1) menționează patru sarcini ale Grupului de lucru care pot fi rezumate ca examinând aplicarea directivei la nivel național în vederea asigurării uniformității și emiterea de avize cu privire la evoluțiile la nivel comunitar: nivelul de protecție, propuneri legislative și coduri de conduită. Această listă evidențiază responsabilitatea largă a Grupului de lucru în domeniul protecției datelor, fapt demonstrat și mai mult în documentele elaborate de Grupul de lucru de-a lungul anilor.

70. Conform comunicării, Grupul de lucru „este un element cheie în asigurarea unei puneri în aplicare mai bune și mai coerente". AEPD subscrie pe deplin la această declarație, dar consideră, de asemenea, necesară clarificarea unor anumite elemente specifice ale responsabilităților.

71. În primul rând, comunicarea îndeamnă la îmbunătățirea contribuției Grupului de lucru, întrucât autoritățile naționale ar trebui să încerce să își adapteze practicile naționale la linia comună ([30]). AEPD salută intenția acestei declarații dar atrage atenția cu privire la confundarea responsabilităților. În conformitate cu articolul 211 CE, Comisia are sarcina de a urmări respectarea directivei în statele membre, inclusiv respectarea acesteia de către autoritățile de supraveghere. Grupul de lucru, în calitate de consultant independent, nu poate fi considerat responsabil pentru aplicarea avizelor sale de către autoritățile naționale.

72. În al doilea rând, Comisia trebuie să fie conștientă de rolurile sale diferite în cadrul Grupului de lucru, deoarece nu este doar membru al Grupului de lucru ci asigură și secretariatul acestuia. În exercitarea celui de-al doilea rol al său, acela de secretar, Comisia trebuie să sprijine Grupul de lucru astfel încât acesta să-și poată desfășura activitatea în mod independent. Aceasta presupune următoarele: Comisia trebuie să asigure resursele necesare și activitatea de secretariat trebuie să se desfășoare conform instrucțiunilor Grupului de lucru și președintelui acestuia, în ceea ce privește conținutul și obiectul activităților Grupului de lucru precum și natura rezultatelor acestuia. În general, activitățile Comisiei în vederea îndeplinirii celorlalte sarcini ale sale, conform legislației CE, nu trebuie să afecteze disponibilitatea sa de a desfășura activități de secretariat.

73. În al treilea rând, deși alegerea priorităților Grupului de lucru este la discreția acestuia, Comisia ar putea indica la ce se așteaptă de la Grupul de lucru și cum consideră că pot fi folosite cel mai eficient resursele disponibile.

74. În al patrulea rând, AEPD regretă faptul că această comunicare nu prevede instrucțiuni clare privind împărțirea rolurilor între Comisie și Grupul de lucru. AEPD invită Comisia să prezinte Grupului de lucru un document care să furnizeze astfel de instrucțiuni. AEPD are următoarele propuneri pentru aspectele ce pot fi abordate în acest document:

— Comisia ar putea invita Grupul de lucru să lucreze pe o serie de aspecte concrete și specificate. Cererile Comisiei ar trebui să se bazeze pe o strategie clară a sarcinilor și priorităților Grupului de lucru,

([30]) A se vedea pagina 11 din comunicare.

— grupul de lucru își stabilește propriile priorități într-un program de lucru cu priorități clare,

— Comisia și Grupul de lucru și-ar putea stabili aranjamentele într-un memorandum de înțelegere,

— este esențial ca Grupul de lucru să se implice pe deplin în interpretarea directivei și să participe la discuțiile care ar putea rezulta în modificarea directivei.

VII. **CONCLUZII**

75. AEPD susține concluzia principală a Comisiei potrivit căreia directiva nu ar trebui să fie modificată pe termen scurt. Această concluzie ar putea fi întărită dacă s-ar fundamenta pe natura directivei și pe politica legislativă a Uniunii.

76. Premisele AEPD sunt:

— pe termen scurt, energia ar trebui folosită în vederea îmbunătățirii punerii în aplicare a directivei,

— pe termen lung, modificarea directivei nu poate fi evitată,

— ar trebui deja să fie stabilită o dată clară pentru a analiza pregătirea propunerilor de modificare. Această dată ar reprezenta un stimulent pentru analizarea viitoarelor modificări.

77. Principalele elemente ale schimbărilor viitoare includ:

— absența necesității de noi principii, dar o nevoie clară de alte aranjamente administrative,

— domeniul extins de aplicare a legislației privind protecția datelor pentru toate utilizările de date cu caracter personal nu ar trebui modificat,

— legislația privind protecția datelor ar trebui să permită o abordare echilibrată în cazuri concrete și ar trebui să permită autorităților pentru protecția datelor să stabilească priorități,

— sistemul ar trebui să se aplice în totalitate utilizării datelor personale pentru aplicarea legii, deși măsuri adecvate suplimentare ar putea fi necesare pentru a aborda problemele speciale din acest domeniu.

78. AEPD propune Comisiei să specifice: un termen pentru activitățile menționate în capitolul 3 al comunicării; un termen pentru un raport ulterior privind aplicarea directivei; specificații privind evaluarea realizării activităților prevăzute; indicații privind modalitățile de acțiune pe termen lung.

79. AEPD salută abordarea privind tehnologia ca un prim pas important și propune începerea discuțiilor privind o abordare pe termen lung, inclusiv, *inter alia*, o dezbatere fundamentală cu privire la dezvoltarea unei societăți de supraveghere. De asemenea, salută revizuirea continuă a Directivei 2002/58/CE și posibila nevoie de norme mai specifice care să abordeze aspectele privind protecția datelor pe care le ridică noile tehnologii, cum ar fi internetul și IDFR. Aceste acțiuni ar trebui să ia în calcul contextul dinamic în întregire și să implice, pe termen lung, și Directiva 95/46/CE.

80. AEPD regretă că perspectiva privind viața privată globală și jurisdicția joacă un rol limitat în comunicare și solicită soluții practice care să reconcilieze nevoia de protecție a persoanelor vizate europene cu limitările teritoriale ale Uniunii Europene și ale statelor membre, cum ar fi: evoluția ulterioară a unui cadru global pentru protecția datelor; evoluția ulterioară a unui regim special pentru transferuri de date către țări terțe; acorduri internaționale privind jurisdicția sau alte acorduri similare cu țări terțe; investiții în mecanisme pentru conformitate globală, cum ar fi utilizarea de reguli corporatiste obligatorii de către societățile multinaționale.

AEPD invită Comisia să inițieze elaborarea unei viziuni în această privință, împreună cu părțile implicate cele mai importante.

81. Referitor la aplicarea legii, AEPD face Comisiei următoarele propuneri:

— să reflecteze în continuare asupra consecințelor implicării societăților private în activități de aplicare a legii,

— să păstreze efectul util al articolului 13 din directivă, propunând, de exemplu, o legislație care să aibă ca scop armonizarea condițiilor și garanțiilor pentru utilizarea derogărilor prevăzute de articolul 13.

82. Aplicarea deplină a directivei presupune: 1. ca statele membre să respecte în totalitate obligațiile proprii prevăzute de legislația europeană și 2. ca alte instrumente, neobligatorii, care ar putea fi esențiale pentru atingerea unui nivel ridicat și armonizat de protecție a datelor să fie utilizate în totalitate. AEPD solicită Comisiei să prezinte cu claritate mijloacele de utilizare a diverselor instrumente și metodele prin care va face distincția între propriile responsabilități și cele ale Grupului de lucru.

83. Referitor la acele instrumente:

— în anumite cazuri, acțiuni legislative specifice ar putea fi necesare la nivel european,

— Comisia este încurajată să urmărească o mai bună punere în aplicarea a directivei, prin proceduri de încălcare,

— Comisia este invitată să utilizeze instrumentul comunicării interpretative — respectând în același timp rolul consultativ al Grupului de lucru și al AEPD — pentru următoarele aspecte: conceptul de date cu caracter personal; definirea rolului operatorului de date sau a persoanei împuternicite de către operator; stabilirea legislației aplicabile; principiul limitării obiectivului și utilizarea incompatibilă; fundamentul juridic pentru prelucrare, în special referitor la consimțământul neechivoc și echilibrul între interese,

— instrumentele neobligatorii să includă instrumentele care să stea la baza conceptului de „viață privată prin concepție" („privacy by design"),

— pe termen lung: acțiuni colective: acțiunile înaintate de persoanele juridice ale căror activități au ca scop protejarea intereselor anumitor categorii de persoane; obligațiile operatorilor de a notifica persoanelor vizate încălcările procedurilor de securitate; dispoziții care să faciliteze utilizarea de mărci de protecție a vieții private sau audituri ale terților părți într-un cadru transnațional.

84. AEPD invită Comisia să prezinte un document Grupului de lucru, prin care să prezinte instrucțiuni clare privind împărțirea rolurilor între Comisie și Grupul de lucru, incluzând următoarele aspecte:

— cererile Comisiei de a lucra pe un număr de aspecte concrete și specifice, în baza unei strategii clare a sarcinilor și priorităților Grupului de lucru,

— posibilitatea de a stabili anumite aranjamente printr-un memorandum de înțelegere,

— implicarea deplină a Grupului de lucru în interpretarea directivei și în discuții care ar putea avea ca rezultat modificarea directivei.

85. Consecințele Tratatului de reformă trebuie luate în considerare pentru a putea asigura aplicarea cât mai extinsă a principiilor de protecție a datelor prevăzute de directivă. AEPD și-a prezentat propunerile într-o scrisoare adresată Președinției CIG.

Adoptată la Bruxelles, 25 iulie 2007.

Peter HUSTINX

Autoritatea Europeană pentru Protecția Datelor