I

(Rezoluții, recomandări și avize)

AVIZE

AUTORITATEA EUROPEANĂ PENTRU PROTECȚIA DATELOR

Avizul Autorității Europene pentru Protecția Datelor privind Comunicarea Comisiei către Parlamentul European, Consiliu, Comitetul Economic și Social și Comitetul Regiunilor – „O abordare globală a protecției datelor cu caracter personal în Uniunea Europeană”

(2011/C 181/01)

AUTORITATEA EUROPEANĂ PENTRU PROTECȚIA DATELOR,

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

având în vedere Carta drepturilor fundamentale a Uniunii Europene, în special articolele 7 și 8,

având în vedere Directiva 95/46/CE a Parlamentului European și a Consiliului din 24 octombrie 1995 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și libera circulație a acestor date [1],

având în vedere 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], în special articolul 41,

ADOPTĂ URMĂTORUL AVIZ:

A. PARTEA GENERALĂ

1. Introducere

1.1. *O primă evaluare generală*

1. La 4 noiembrie 2010, Comisia a adoptat o comunicare intitulată „O abordare globală a protecției datelor cu caracter personal în Uniunea Europeană” („Comunicarea”) [3]. Comunicarea a fost trimisă spre consultare Autorității Europene pentru Protecția Datelor (AEPD). AEPD salută faptul că a fost consultată de Comisie, în conformitate cu articolul 41 din Regulamentul (CE) nr. 45/2001. Anterior adoptării Comunicării, AEPD îi fusese deja oferită posibilitatea de a prezenta observații neoficiale, unele dintre acestea fiind luate în considerare în versiunea finală a documentului.

2. Comunicarea își propune să definească abordarea Comisiei privind revizuirea sistemului juridic al UE în materie de protecție a datelor cu caracter personal în toate domeniile de activitate ale Uniunii, ținând seama, în special, de provocările pe care le ridică globalizarea și noile tehnologii [4].

3. În general, AEPD salută Comunicarea, fiind convinsă de necesitatea unei revizuiri a cadrului juridic actual în materie de protecție a datelor în UE, în scopul asigurării unei protecții eficiente într-o societate informațională în continuă dezvoltare. În Avizul din 25 iulie 2007 referitor la punerea în aplicare a Directivei privind protecția datelor [5], AEPD concluziona că, pe termen lung, modificarea Directivei 95/46/CE nu poate fi evitată.

4. Comunicarea reprezintă un pas important în direcția unei asemenea modificări legislative care, la rândul său, ar constitui cea mai importantă evoluție în domeniul protecției datelor în UE de la adoptarea Directivei 95/46/CE, care este considerată, în general, piatra de temelie a protecției datelor în cadrul Uniunii Europene (precum și la nivel mai larg în Spațiul Economic European).

5. Comunicarea oferă cadrul adecvat pentru o revizuire bine orientată, identificând, de asemenea, într-o manieră generală, principalele probleme și provocări. AEPD împărtășește opinia Comisiei potrivit căreia în viitor va fi, totuși, necesar un sistem solid de protecție a datelor, în baza faptului că principiile generale existente de protecție a datelor sunt încă valabile într-o societate ce suferă schimbări fundamentale datorate dezvoltării tehnologice rapide și globalizării. Acest lucru impune revizuirea dispozițiilor legislative existente.

[1] JO L 281, 23.11.1995, p. 31.
[2] JO L 8, 12.1.2001, p. 1.
[3] COM(2010) 609 final.
[4] A se vedea p. 5, primul paragraf din Comunicare.
[5] Avizul AEPD din 25 iulie 2007 privind Comunicarea Comisiei către Parlamentul European și Consiliu cu privire la continuarea programului de lucru pentru o mai bună punere în aplicare a Directivei privind protecția datelor (JO C 255, 27.10.2007, p. 1).

6. Comunicarea subliniază în mod corect faptul că provocările sunt enorme. AEPD împărtășește pe deplin această afirmație și scoate în evidență necesitatea ca soluțiile propuse să fie pe măsură de ambițioase și să sporească eficiența protecției.

1.2. *Scopul avizului*

7. Prezentul aviz evaluează soluțiile propuse în Comunicare pe baza următoarelor două criterii: ambiție și eficiență. Perspectiva avizului este, în general, pozitivă. AEPD sprijină Comunicarea, însă critică, în același timp, aspectele în care mai multă ambiție, în opinia sa, ar conduce la un sistem mai eficient.

8. AEPD are drept scop să contribuie, prin prezentul aviz, la dezvoltarea în continuare a cadrului juridic în materie de protecție a datelor. AEPD așteaptă cu interes propunerea Comisiei, preconizată a fi prezentată până la jumătatea anului 2011, și speră că sugestiile sale vor fi luate în considerare la elaborarea acestei propuneri. De asemenea, AEPD menționează că această Comunicare pare să excludă anumite domenii din instrumentul general, de exemplu, prelucrarea datelor de către instituțiile și organismele UE. În cazul în care Comisia ar decide, într-adevăr, să elimine anumite domenii în această etapă, ceea ce AEPD ar considera regretabil, aceasta din urmă îndeamnă Comisia să se angajeze în construirea unei arhitecturi globale, într-un interval de timp scurt, specificat.

1.3. *Elementele fundamentale ale prezentului aviz*

9. Prezentul aviz nu este independent, ci se bazează pe poziții anterioare adoptate, în diverse ocazii, de AEPD și de autoritățile de protecție a datelor din Europa. În mod special, trebuie subliniat faptul că în avizul AEPD din 25 iulie 2007, menționat deja, au fost identificate și prezentate în detaliu unele elemente principale ale modificării viitoare ([6]). De asemenea, avizul se bazează pe discuțiile cu alte părți interesate din domeniul protecției datelor și a vieții private. Contribuțiile acestor discuții au constituit un fundament util atât pentru Comunicare, cât și pentru prezentul aviz. În acest sens, se poate concluziona că există un anumit nivel de sinergie în ceea ce privește modalitățile de îmbunătățire a eficienței protecției datelor.

10. Un alt element fundamental al prezentului aviz îl constituie documentul intitulat „Viitorul vieții private", contribuție comună a Grupului de lucru instituit în temeiul articolului 29 și a Grupului de lucru pentru poliție și justiție la consultarea lansată de Comisie în 2009 („documentul Grupului de lucru privind viitorul vieții private") ([7]).

11. Mai recent, la conferința de presă din 15 noiembrie 2010, AEPD a prezentat primele sale reacții față de această Comunicare. Prezentul aviz dezvoltă opiniile mai generale exprimate în timpul acestei conferințe de presă ([8]).

12. În sfârșit, prezentul aviz se bazează pe o serie de avize anterioare ale AEPD, precum și pe documente ale Grupului de lucru privind protecția datelor instituit în temeiul articolului 29. Prezentul aviz face trimitere, atunci când este relevant, la aceste avize și documente.

2. **Context**

13. Revizuirea normelor privind protecția datelor se desfășoară într-un moment istoric crucial. Comunicarea prezintă contextul pe larg și într-o manieră convingătoare. Pe baza acestei descrieri, AEPD identifică cei patru factori principali care determină mediul în care se desfășoară procesul de revizuire.

14. Primul factor îl constituie dezvoltarea tehnologică. Tehnologia de astăzi nu este aceeași cu cea din momentul conceperii și adoptării Directivei 95/46/CE. Fenomenele tehnologice precum „cloud computing", publicitatea comportamentală, rețelele de socializare, dispozitivele de colectare a taxei de drum și de localizare geografică au modificat profund modalitatea de prelucrare a datelor și creează reale probleme în ceea ce privește protecția datelor. Revizuirea normelor europene de protecție a datelor va trebui să abordeze în mod eficient aceste provocări.

15. Al doilea factor este globalizarea. Eliminarea treptată a barierelor comerciale a oferit întreprinderilor o dimensiune internațională din ce în ce mai amplă. Prelucrarea transfrontalieră a datelor și transferurile internaționale de date au cunoscut o creștere uriașă în ultimii ani. Mai mult decât atât, prelucrarea datelor s-a generalizat datorită tehnologiilor informației și comunicațiilor: internetul și „cloud computing" au permis prelucrarea delocalizată a unor cantități mari de date la scară mondială. De asemenea, ultimul deceniu a cunoscut o intensificare a activităților polițienești și judiciare internaționale de combatere a terorismului și a altor forme de

([6]) În mod special (a se vedea punctul 77 din aviz): absența necesității modificării principiilor existente, dar o nevoie clară de alte dispoziții 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 cu caracter personal pentru aplicarea legii, deși măsuri adecvate suplimentare ar putea fi necesare pentru a aborda problemele speciale din acest domeniu.

([7]) Documentul 168 al Grupului de lucru (http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp168_en.pdf). Mesajul său principal este că o modificare legislativă reprezintă o bună ocazie de a clarifica unele norme și principii esențiale (de exemplu, consimțământul, transparența), de a introduce unele principii noi (de exemplu, confidențialitatea prin concept, responsabilitatea), de a spori eficiența prin modernizarea dispozițiilor (de exemplu, prin limitarea cerințelor de notificare existente) și de a include totul într-un cadru juridic complet (inclusiv cooperarea polițienească și judiciară).

([8]) Punctele de discuție pentru conferința de presă sunt disponibile pe site-ul internet al AEPD la adresa: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2010/10-11-15_Press_conf_speaking_points_PHBG_EN.pdf

crimă organizată internațională, sprijinite printr-un volum imens de schimburi de informații în scopul aplicării legii. Toate acestea necesită o analiză profundă a modului în care protecția datelor cu caracter personal poate fi efectiv asigurată într-o lume globalizată, fără a afecta substanțial activitățile de prelucrare internaționale.

16. Cel de al treilea factor îl constituie Tratatul de la Lisabona. Intrarea în vigoare a Tratatului de la Lisabona marchează o nouă eră pentru protecția datelor. Articolul 16 din TFUE nu prevede doar dreptul individual al persoanei vizate, ci și un temei juridic direct pentru o legislație puternică a protecției datelor în UE. Mai mult decât atât, eliminarea structurii bazate pe piloni obligă Parlamentul European și Consiliul să prevadă protecția datelor în toate domeniile dreptului comunitar. Cu alte cuvinte, acest lucru permite un cadru juridic global în materie de protecție a datelor, aplicabil sectorului privat, sectorului public din statele membre, precum și instituțiilor și organismelor UE. În acest sens, Programul de la Stockholm ([9]) prevede în mod constant faptul că Uniunea trebuie să asigure o strategie globală pentru protecția datelor în cadrul UE și al relațiilor acesteia cu alte țări.

17. Al patrulea factor îl constituie evoluțiile paralele care au loc în contextul organizațiilor internaționale. În prezent se desfășoară diverse dezbateri concentrate pe modernizarea actualelor instrumente juridice pentru protecția datelor. În acest sens, este important să se menționeze actualele reflecții legate de viitoarea revizuire a Convenției nr. 108 a Consiliului Europei ([10]) și a Orientărilor OCDE privind viața privată ([11]). O altă evoluție importantă se referă la adoptarea de standarde internaționale privind protecția datelor cu caracter personal și a vieții private, ceea ce ar putea duce la adoptarea unui instrument global obligatoriu pentru protecția datelor. Toate aceste inițiative merită a fi sprijinite în totalitate. Scopul lor comun ar trebui să fie asigurarea protecției eficiente și coerente într-un mediu bazat pe tehnologie și globalizat.

3. **Perspective principale**

3.1. *Protecția datelor consolidează încrederea și trebuie să sprijine alte interese (publice)*

18. Un cadru juridic solid privind protecția datelor reprezintă consecința necesară a importanței acordate protecției datelor în Tratatul de la Lisabona, în special la articolul 8 din Carta drepturilor fundamentale a Uniunii și articolul 16 din Tratatul privind funcționarea Uniunii Europene (TFUE), precum și consecința legăturii puternice cu articolul 7 din Cartă ([12]).

19. Însă un cadru juridic solid privind protecția datelor servește, de asemenea, unui public mai larg și intereselor private dintr-o societate informațională în care prelucrarea datelor este generalizată. Protecția datelor consolidează încrederea, aceasta constituind o componentă esențială a bunei funcționări a societății noastre. Este esențial ca dispozițiile privind protecția datelor să fie concepute în așa fel încât, în măsura posibilului, acestea să sprijine în mod activ, nu să afecteze alte drepturi și interese legitime.

20. O economie europeană puternică, securitatea persoanelor, precum și responsabilitatea guvernelor constituie exemple importante de alte interese legitime.

21. Dezvoltarea economică în UE este strâns legată de introducerea și comercializarea de noi tehnologii și servicii. În societatea informațională, introducerea și dezvoltarea cu succes a tehnologiilor informațiilor și comunicațiilor (TIC), precum și a serviciilor se bazează pe încredere. Dacă oamenii nu au încredere în TIC, aceste tehnologii au șanse mici de reușită ([13]), iar oamenii vor avea încredere în TIC numai dacă datele lor sunt protejate în mod eficient. Prin urmare, protecția datelor ar trebui să constituie parte integrantă a tehnologiilor și serviciilor. Un cadru juridic solid în materie de protecție a datelor promovează economia europeană, cu condiția ca acesta să fie nu doar solid, ci și adaptat în mod corespunzător. În acest sens, mai buna armonizare în cadrul UE și reducerea la minimum a sarcinilor administrative sunt esențiale (a se vedea capitolul 5 din prezentul aviz).

22. În ultimii ani s-a vorbit mult despre necesitatea echilibrului dintre confidențialitate și securitate, în special în ceea ce privește instrumentele de prelucrare și schimb de date care au loc în cadrul cooperării polițienești și judiciare ([14]). Protecția datelor a fost adesea în mod greșit caracterizată ca fiind un obstacol în calea protejării depline a securității fizice a persoanelor fizice ([15]) sau cel puțin o condiție inevitabilă care trebuie respectată de autoritățile de aplicare a legii. Această caracterizare, însă, nu este tot. Un cadru juridic solid în materie de protecție a datelor poate intensifica și consolida securitatea. Pe baza principiilor privind protecția datelor, atunci când aceste principii sunt corect aplicate, operatorii sunt obligați să se asigure că informațiile sunt exacte și actualizate și că datele cu caracter personal care sunt inutile pentru aplicarea legii sunt eliminate din sisteme. De asemenea, se pot invoca obligațiile de punere în aplicare a măsurilor de natură tehnologică și organizațională pentru a asigura securitatea sistemelor, cum ar fi

([9]) Programul de la Stockholm – O Europă deschisă și sigură în serviciul cetățenilor și pentru protecția acestora (JO C 115, 4.5.2010, p. 1), la p. 10.

([10]) Convenția nr. 108 a Consiliului Europei pentru protecția persoanelor fizice în ceea ce privește prelucrarea automatizată a datelor cu caracter personal, STE nr. 108, 28 ianuarie 1981.

([11]) Orientările OCDE privind protecția confidențialității și fluxurile transfrontaliere de date cu caracter personal, publicate pe site-ul internet: http://www.oecd.org

([12]) Această importanță a protecției datelor și legătura cu viața privată, exprimate în Cartă, au fost subliniate de Curtea de Justiție în Hotărârea din 9 noiembrie 2010 pronunțată în cauzele conexe C-92/09 și C-93/09, *Schecke*, nepublicată încă în Culegere.

([13]) A se vedea Avizul AEPD din 18 martie 2010 privind promovarea încrederii în societatea informațională prin încurajarea protecției datelor și a confidențialității (JO C 280, 16.10.2010, p. 1), punctul 113.

([14]) A se vedea, de exemplu, Avizul AEPD din 10 iulie 2009 privind Comunicarea Comisiei către Parlamentul European și Consiliu – „Un spațiu de libertate, securitate și justiție în serviciul cetățenilor” (JO C 276, 17.9.2009, p. 8).

([15]) Noțiunea de securitate este mai largă decât noțiunea de securitate fizică, însă ca ilustrare a argumentelor prezentate, este utilizată aici în sensul său mai restrâns.

protejarea sistemelor împotriva divulgării sau accesului neautorizat, astfel cum acestea au fost elaborate în domeniul protecției datelor.

23. Respectarea principiilor privind protecția datelor poate asigura în continuare faptul că autoritățile de aplicare a legii acționează în conformitate cu principiile statului de drept, care atrage încrederea în comportamentul acestora și, prin urmare, promovează, în sens mai larg, încrederea în societățile noastre. Jurisprudența prezentată la articolul 8 din Convenția Europeană a Drepturilor Omului asigură faptul că autoritățile polițienești și judiciare pot prelucra toate datele relevante pentru activitatea lor, însă nu în mod nelimitat. Protecția datelor necesită un mecanism de verificare și control (a se vedea capitolul 9 din aviz referitor la poliție și justiție).

24. În societățile democratice, guvernele sunt responsabile de toate activitățile lor, inclusiv de utilizarea datelor cu caracter personal pentru diferitele interese publice pe care le servesc. Aceste interese variază de la publicarea datelor pe internet, din motive de transparență, până la utilizarea datelor ca suport pentru politici în domenii precum sănătatea publică, transporturile sau fiscalitatea, sau supravegherea persoanelor în scopul aplicării legii. Un cadru juridic solid privind protecția datelor permite guvernelor să își respecte responsabilitățile și să fie responsabile, ca parte a bunei guvernanțe.

3.2. *Consecințele asupra cadrului juridic în materie de protecție a datelor*

3.2.1. Este necesară o mai bună armonizare

25. Comunicarea a identificat în mod corect faptul că una dintre lacunele cadrului juridic actual este că acordă prea multă libertate statelor membre în privința punerii în aplicare a dispozițiilor europene în legislația națională. Lipsa armonizării are o serie de consecințe negative într-o societate informațională în care granițele fizice dintre statele membre sunt din ce în ce mai puțin relevante (a se vedea capitolul 5 din prezentul aviz).

3.2.2. Principiile generale privind protecția datelor rămân valabile

26. Un prim motiv mai oficial pentru care principiile generale privind protecția datelor nu ar trebui și nu ar putea fi modificate este de natură juridică. Aceste principii sunt stabilite în Convenția nr. 108 a Consiliului Europei, care este obligatorie pentru toate statele membre. Această convenție reprezintă temeiul protecției datelor în UE. De asemenea, unele dintre principiile esențiale sunt în mod explicit prezentate în articolul 8 din Carta drepturilor fundamentale a Uniunii. Prin urmare, modificarea acestor principii ar necesita modificarea tratatelor.

27. În realitate, însă, există și motive substanțiale de a nu modifica principiile generale. AEPD este convinsă că o societate informațională nu poate și nu ar trebui să funcționeze fără o protecție adecvată a vieții private și a datelor cu caracter personal ale persoanelor fizice. De asemenea, atunci când se prelucrează mai multe informații, este necesară o mai bună protecție. O societate informațională în care sunt prelucrate volume uriașe de informații legate de orice persoană trebuie să se bazeze pe conceptul de control din partea persoanei, pentru a permite acesteia să acționeze ca persoană fizică și să își exercite libertățile într-o societate democratică, precum libertatea de expresie și a cuvântului.

28. De asemenea, este dificil de imaginat controlul exercitat de o persoană fără obligația operatorilor de a limita prelucrarea în conformitate cu principiile necesității, proporționalității și limitării scopului. La fel de dificil este de imaginat controlul exercitat de o persoană în lipsa recunoașterii drepturilor persoanelor vizate, precum dreptul de acces, rectificare, ștergere sau blocare a datelor.

3.2.3. Perspectiva drepturilor fundamentale

29. AEPD subliniază faptul că protecția datelor este recunoscută ca drept fundamental. Acest lucru nu înseamnă că protecția datelor ar trebui întotdeauna să *prevaleze* asupra altor drepturi și interese importante într-o societate democratică, ci că are, într-adevăr, consecințe asupra naturii și sferei de aplicare a protecției care trebuie acordată în temeiul unui cadru juridic european, astfel încât să se țină seama întotdeauna și în mod corespunzător de cerințele referitoare la protecția datelor.

30. Aceste principale consecințe pot fi definite după cum urmează:

— protecția trebuie să fie eficientă. Un cadru juridic trebuie să prevadă instrumente care să permită persoanelor fizice să își exercite drepturile în practică;

— cadrul juridic trebuie să fie stabil pentru o perioadă lungă de timp;

— protecția trebuie acordată în toate circumstanțele și să nu depindă de preferințele politice dintr-o anumită perioadă;

— limitarea exercitării dreptului poate fi necesară, însă trebuie să fie excepțională, justificată în mod corespunzător și să nu afecteze niciodată elementele esențiale ale dreptului propriu-zis ([16]).

AEPD recomandă Comisiei să țină seama de aceste consecințe în propunerile sale de soluții legislative.

3.2.4. Sunt necesare noi dispoziții legislative

31. Comunicarea se axează în mod justificat pe necesitatea consolidării dispozițiilor legislative privind protecția datelor. În acest context, se cuvine să amintim că în documentul Grupului de lucru privind viitorul vieții private ([17]), autoritățile de protecție a datelor au subliniat necesitatea

([16]) A se vedea, de asemenea, Avizul AEPD din 25 iulie 2007 privind Comunicarea Comisiei către Parlamentul European și Consiliu cu privire la continuarea programului de lucru pentru o mai bună punere în aplicare a Directivei privind protecția datelor, paragraful 17, care se bazează pe jurisprudența Curții Europene a Drepturilor Omului și a Curții de Justiție.

([17]) A se vedea nota de subsol nr. 7.

ca diferiții actori din domeniul protecției datelor, în special persoanele vizate, operatorii de date și autoritățile de supraveghere propriu-zise să joace un rol mai important.

32. Se pare că există un larg consens în rândul părților interesate în ceea ce privește faptul că dispozițiile legislative mai solide, care țin seama de dezvoltările tehnologice și de globalizare, reprezintă în viitor cheia unei protecții ambițioase și eficiente a datelor. Astfel cum s-a menționat deja la punctul 7, acestea sunt criteriile AEPD de evaluare a oricăror soluții propuse.

3.2.5. Completitudinea ca o condiție indispensabilă

33. Astfel cum se menționează în Comunicare, Directiva 95/46/CE se aplică tuturor activităților de prelucrare a datelor cu caracter personal desfășurate în statele membre, atât în sectorul public, cât și în cel privat, cu excepția activităților care nu intră în sfera de aplicare a dreptului comunitar anterior ([18]). Deși în fostul tratat această excepție era necesară, după intrarea în vigoare a Tratatului de la Lisabona ea nu se mai aplică. În plus, excepția este contrară textului, nefiind, în orice caz, în spiritul articolului 16 din TFUE.

34. În opinia AEPD, un instrument juridic complet pentru protecția datelor, incluzând o cooperare polițienească și juridică în materie penală, trebuie privit ca una dintre principalele îmbunătățiri pe care le poate aduce un nou cadru juridic. Aceasta constituie o condiție indispensabilă pentru protecția eficientă a datelor în viitor.

35. În sprijinul acestei afirmații, AEPD scoate în evidență următoarele argumente:

— deosebirea dintre activitățile sectorului privat și ale sectorului de aplicare a legii tinde să se atenueze. Entitățile din sectorul privat pot prelucra date care în ultimă instanță sunt folosite în scopul aplicării legii (exemplu: datele din PNR ([19])), în timp ce, în alte cazuri, ele sunt obligate să păstreze datele pentru scopuri de aplicare a legii (exemplu: Directiva privind păstrarea datelor ([20]));

— conform Directivei 95/46/CE, nu există nicio diferență fundamentală între autoritățile polițienești și judiciare și alte autorități care asigură aplicarea legii (fiscale, vamale, antifraudă, de imigrație);

— astfel cum se descrie cu exactitate în Comunicare, instrumentul juridic pentru protecția datelor aplicabil în prezent autorităților polițienești și judiciare (Decizia-cadru 2008/977/JAI ([21])) este inadecvat;

— majoritatea statelor membre au transpus în legislațiile naționale atât Directiva 95/46/CE, cât și Convenția nr. 108, făcându-le aplicabile și autorităților lor polițienești și judiciare.

36. Includerea poliției și justiției în instrumentul juridic general ar însemna nu doar oferirea mai multor garanții cetățenilor, ci și ușurarea sarcinii autorităților polițienești. Obligația de a aplica diverse seturi de norme este greoaie, necesitând un consum inutil de timp și ridicând obstacole în calea cooperării internaționale (a se vedea, în continuare, capitolul 9 din prezentul aviz). De asemenea, acesta constituie un argument pentru includerea activităților de prelucrare de către serviciile de securitate naționale, în măsura în care acest lucru este posibil în stadiul actual al legislației UE.

3.2.6. Neutralitate tehnologică

37. Perioada scursă de la adoptarea, în 1995, a Directivei 95/46/CE poate fi caracterizată ca o perioadă turbulentă din punct de vedere tehnologic. În mod frecvent sunt introduse noi dezvoltări și dispozitive tehnologice. În multe cazuri acest lucru a dus la modificări fundamentale ale modului de prelucrare a datelor cu caracter personal ale persoanelor fizice. Societatea informațională nu mai poate fi considerată un mediu paralel, la care cetățenii pot participa în mod voluntar, ci a devenit o parte integrantă a vieții noastre de zi cu zi. De exemplu, conceptul de internet al obiectelor ([22]) stabilește legături între obiectele fizice și informațiile on-line referitoare la acestea.

38. Tehnologia va continua să se dezvolte, ceea ce va avea consecințe asupra noului cadru juridic care trebuie să fie eficace pentru o perioadă lungă de timp, dar, totodată, să nu împiedice dezvoltările tehnologice viitoare. Astfel, este necesar ca dispozițiile legislative să fie neutre din punct de vedere tehnologic. Cu toate acestea, cadrul juridic trebuie să ofere o mai bună securitate juridică întreprinderilor și persoanelor fizice, care trebuie să înțeleagă ce se așteaptă de la ele și să își să poată exercita drepturile. Prin urmare, este necesar ca dispozițiile legislative să fie precise.

39. Potrivit AEPD, un instrument juridic general pentru protecția datelor trebuie formulat, pe cât posibil, într-o manieră neutră din punct de vedere tehnologic, ceea ce înseamnă că drepturile și obligațiile diferiților actori trebuie formulate într-o manieră generală și neutră, astfel încât să rămână, în principiu, valabile și aplicabile indiferent de tehnologia aleasă în scopul prelucrării datelor cu caracter personal. Nu există altă posibilitate, dat fiind

([18]) Prezentul aviz se va axa, în principal, pe fostul pilon 3 (cooperarea polițienească și judiciară în materie penală), pilonul 2 fiind nu doar un domeniu mai complicat al dreptului comunitar (după cum se admite în articolul 16 din TFUE și articolul 39 din TFUE), ci și mai puțin relevant pentru prelucrarea datelor.

([19]) A se vedea, de exemplu, Comunicarea Comisiei privind o abordare globală referitoare la transferul de date din registrul cu numele pasagerilor (*Passenger Name Record*, PNR) către țările terțe, COM(2010) 492 final.

([20]) 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).

([21]) Decizia-cadru 2008/977/JAI a Consiliului din 27 noiembrie 2008 privind protecția datelor cu caracter personal prelucrate în cadrul cooperării polițienești și judiciare în materie penală (JO L 350, 30.12.2008, p. 60).

([22]) Astfel cum este definit în „Internetul obiectelor – un plan de acțiune pentru Europa", COM(2009) 278 final.

ritmul progreselor tehnologice din zilele noastre. AEPD propune introducerea de noi drepturi „neutre din punct de vedere tehnologic" care să se situeze deasupra principiilor existente privind protecția datelor și care ar putea avea o importanță specială în mediul electronic aflat într-o evoluție rapidă (a se vedea, în special, capitolele 6 și 7).

3.2.7. Pe termen lung: securitate juridică pentru o perioadă mai lungă de timp

40. În ultimii 15 ani, Directiva 95/46/CE a reprezentat elementul central al protecției datelor în UE, fiind transpusă în legislațiile statelor membre și aplicată de diferiții actori. În timp, punerea în aplicare s-a îmbunătățit pe baza experiențelor practice și a orientărilor ulterioare emise de Comisie, de autoritățile pentru protecția datelor (la nivel național și în cadrul Grupului de lucru instituit în temeiul articolului 29) și de instanțele naționale și europene.

41. Merită subliniat faptul că aceste dezvoltări necesită timp și că fiind, mai ales, vorba de un cadru juridic general care instituie un drept fundamental, acest timp este necesar pentru a crea securitate juridică și stabilitate. Noul instrument juridic general trebuie elaborat cu ambiția ca acesta să fie capabil să creeze securitate juridică și stabilitate pentru o perioadă mai lungă de timp, ținând seama de faptul că este foarte greu de prevăzut modul în care tehnologia și globalizarea vor evolua ulterior. În orice caz, AEPD sprijină pe deplin scopul creării securității juridice pentru o perioadă mai lungă de timp, comparabil cu perspectiva Directivei 95/46/CE. Pe scurt, deși tehnologia evoluează rapid, legislația trebuie să fie stabilă.

3.2.8. Pe termen scurt: eficientizarea utilizării instrumentelor existente

42. Pe termen scurt, este esențial să se asigure eficacitatea dispozițiilor legislative existente, în primul rând prin concentrarea pe aplicarea legii, atât la nivel național, cât și la nivelul UE (a se vedea capitolul 11 din prezentul aviz).

B. ELEMENTELE NOULUI CADRU JURIDIC

4. Abordarea globală

43. AEPD sprijină pe deplin abordarea globală a protecției datelor, care reprezintă nu doar titlul, ci și punctul de plecare al Comunicării și care include neapărat extinderea normelor generale privind protecția datelor la cooperarea polițienească și judiciară în materie penală ([23]).

44. Cu toate acestea, AEPD menționează că intenția Comisiei nu este aceea de a include toate activitățile de prelucrare a datelor în acest instrument juridic general. Mai precis, prelucrarea datelor de către instituțiile, organismele, birourile și agențiile UE nu va fi inclusă. Comisia afirmă doar că „va evalua necesitatea adaptării altor instrumente juridice la noul cadru general privind protecția datelor".

45. În mod clar, AEPD preferă includerea în cadrul juridic general a prelucrării datelor la nivelul UE. AEPD amintește faptul că aceasta fusese intenția inițială a fostului articol 286 din Tratatul CE, în care protecția datelor era menționată prima dată la nivelul tratatului. Articolul 286 din Tratatul CE prevedea doar că instrumentele juridice privind prelucrarea datelor cu caracter personal se vor aplica și instituțiilor. Mai important, un text legislativ unic evită riscul discrepanțelor dintre dispoziții și ar fi mai adecvat pentru schimbul de date efectuat între entitățile de la nivelul UE și entitățile publice și private din statele membre. De asemenea, acest text unic ar evita riscul ca, după modificarea Directivei 95/46/CE, să nu mai existe interes politic în modificarea Regulamentului (CE) nr. 45/2001 sau acordarea unei priorități suficiente acestei modificări pentru a evita discrepanțele între datele intrării în vigoare.

46. AEPD invită Comisia, în cazul în care ar concluziona că includerea în instrumentul juridic general a prelucrării datelor la nivelul UE nu ar fi fezabilă, să se angajeze să propună o adaptare a Regulamentului (CE) nr. 45/2001 (nu să „evalueze necesitatea") în cel mai scurt timp posibil, de preferință, până la sfârșitul anului 2011.

47. La fel de importantă este asigurarea, de către Comisie, a faptului că nu sunt omise alte domenii, în special:

— protecția datelor în cadrul Politicii externe și de securitate comună, în temeiul articolului 39 din TUE ([24]);

— regimurile sectoriale de protecție a datelor pentru organisme UE precum Europol, Eurojust și pentru sisteme informaționale la scară largă, în măsura în care acestea necesită a fi adaptate la noul instrument juridic;

— Directiva 2002/58 asupra confidențialității și comunicațiilor electronice (Directiva ePrivacy), în măsura în care aceasta necesită a fi adaptată la noul instrument juridic.

48. În sfârșit, instrumentul juridic general pentru protecția datelor poate și probabil trebuie să fie completat de reglementări sectoriale și specifice suplimentare, de exemplu, în domeniul cooperării polițienești și judiciare, dar și în alte domenii ([25]). Atunci când este necesar și în conformitate cu principiul subsidiarității, aceste reglementări suplimentare ar trebui adoptate la nivelul UE. Statele membre pot elabora norme suplimentare în domenii specifice, dacă acest lucru este justificat (a se vedea secțiunea 5.2).

([23]) A se vedea p. 14 din Comunicare și secțiunea 3.2.5 din prezentul aviz.

([24]) A se vedea, de asemenea, Avizul AEPD din 24 noiembrie 2010 privind Comunicarea Comisiei către Parlamentul European și Consiliu cu privire la Politica UE de combatere a terorismului: principale realizări și viitoare provocări, paragraful 31.

([25]) A se vedea, de asemenea, documentul GL privind viitorul vieții private (nota de subsol 7), punctele 18-21.

5. **Mai buna armonizare și simplificare**

5.1. *Necesitatea armonizării*

49. Armonizarea este extrem de importantă pentru legislația UE privind protecția datelor. Comunicarea a subliniat în mod just faptul că protecția datelor are o puternică dimensiune a pieței interne, deoarece trebuie să asigure fluxul liber de date cu caracter personal între statele membre în cadrul pieței interne. Cu toate acestea, nivelul de armonizare prevăzut de directiva actuală a fost considerat ca fiind mai puțin satisfăcător. Comunicarea confirmă faptul că aceasta este una dintre principalele preocupări recurente ale părților interesate. În special, părțile interesate scot în evidență necesitatea consolidării securității juridice, a reducerii sarcinii administrative și a asigurării unor condiții de concurență echitabile pentru operatorii economici. Astfel cum în mod corect menționează Comisia, acesta este, îndeosebi, cazul operatorilor de date stabiliți în mai multe state membre, care sunt obligați să respecte cerințele (posibil divergente) ale legislațiilor naționale privind protecția datelor ([26]).

50. Armonizarea nu este importantă doar pentru piața internă, ci și pentru asigurarea unei protecții adecvate a datelor. Articolul 16 din TFUE prevede că „fiecare” are dreptul la protecția datelor sale cu caracter personal. Pentru ca acest drept să fie efectiv respectat, este necesar ca, pe întreg teritoriul UE, să fie garantat un nivel echivalent de protecție. Documentul Grupului de lucru (GL) pentru viitorul vieții private a subliniat că mai multe dispoziții referitoare la pozițiile persoanelor vizate nu au fost puse în aplicare sau interpretate în mod uniform în toate statele membre ([27]). Într-o societate globalizată și inter-relaționată, aceste divergențe ar putea submina sau limita protecția persoanelor fizice.

51. AEPD consideră că mai buna armonizare reprezintă unul dintre principalele obiective ale procesului de revizuire. AEPD salută angajamentul Comisiei de a analiza mijloacele de realizare a unei mai bune armonizări a protecției datelor la nivelul UE. Cu toate acestea, AEPD menționează cu oarecare surprindere că această Comunicare nu prezintă, în acest stadiu, nicio opțiune concretă. Prin urmare, AEPD este cea care indică unele domenii în care o mai bună convergență constituie o urgență (a se vedea secțiunea 5.3). Mai buna armonizare în aceste domenii nu ar trebui realizată numai prin reducerea marjei de manevră a legislației naționale, ci și prin prevenirea implementării incorecte de către statele membre (a se vedea capitolul 11) și asigurarea aplicării mai consecvente și mai coordonate (a se vedea, de asemenea, capitolul 10).

([26]) Comunicarea, p. 10.

([27]) A se vedea documentul GL privind viitorul vieții private (nota de subsol 7), punctul 70. Documentul face referire, în special, la dispozițiile privind răspunderea și la posibilitatea de a pretinde daune imateriale.

5.2. *Reducerea marjei de manevră în ceea ce privește aplicarea directivei*

52. Directiva conține o serie de dispoziții formulate într-o manieră generală, care lasă suficient loc de divergențe în ceea ce privește punerea lor în aplicare. Considerentul 9 din directivă confirmă în mod explicit faptul că statelor membre le este acordată o anumită marjă de manevră și că, în limitele acesteia, pot apărea discrepanțe în punerea în aplicare a directivei. Mai multe dispoziții au fost puse în aplicare în mod diferit de statele membre, inclusiv unele dispoziții esențiale ([28]). Această situație este nesatisfăcătoare și ar trebui să se urmărească o mai bună convergență.

53. Aceasta nu înseamnă că diversitatea ar trebui exclusă în mod direct. În anumite domenii ar putea fi nevoie de flexibilitate pentru a menține caracteristicile justificate, interesele publice importante sau autonomia instituțională a statelor membre. Potrivit AEPD, posibilitatea existenței divergențelor între statele membre ar trebui limitată, în special, la următoarele situații specifice:

— libertatea de exprimare: potrivit cadrului juridic actual (articolul 9), statele membre pot prevede exonerări și derogări pentru prelucrarea datelor efectuată în scopuri jurnalistice, artistice sau literare. Această flexibilitate pare îndreptățită, desigur, sub rezerva limitelor prevăzute de Cartă și de CEDO, având în vedere tradițiile diferite și diferențele culturale care pot exista în statele membre în acest domeniu. Totuși, acest lucru nu va împiedica o posibilă actualizare a actualului articol 9 în lumina evoluțiilor internetului;

— interesele publice specifice: potrivit cadrului juridic actual (articolul 13), statele membre pot adopta măsuri legislative pentru a restrânge domeniul obligațiilor și drepturilor dacă o astfel de restricție constituie o măsură necesară pentru a proteja interesele publice importante, precum securitatea statului, apărarea, securitatea publică etc. Această competență a statelor membre rămâne justificată, însă, dacă este posibil, interpretarea excepțiilor ar trebui mai bine armonizată (a se vedea secțiunea 9.1). În plus, domeniul actual al exceptării de la dispozițiile articolului 6 alineatul (1) pare nejustificat de largă;

— căile de atac, sancțiunile și procedurile administrative: un cadru juridic european ar trebui să stabilească principalele condiții, însă, potrivit legislației actuale a UE, stabilirea sancțiunilor, a căilor de atac, a normelor procedurale și mijloacele de anchetă aplicabile la nivel național trebuie să rămână în competența statelor membre.

([28]) În privința datelor manuale, există, de asemenea, mai multe abordări divergente.

5.3. *Domenii care necesită o mai bună armonizare*

54. *Definiții* (articolul 2 din Directiva 95/46/CE). Definițiile constituie piatra de temelie a sistemului juridic și ar trebui să fie interpretate în mod uniform în toate statele membre, fără nicio libertate în ceea ce privește punerea în aplicare. În cadrul actual au apărut divergențe legate, de exemplu, de noțiunea de operator ([29]). AEPD propune adăugarea unor elemente suplimentare pe lista actuală inclusă la articolul 2, pentru a oferi o mai bună securitate juridică, de exemplu, date anonime, date sub pseudonim, date cu caracter judiciar, transfer de date și responsabil cu protecția datelor.

55. *Legalitatea prelucrării (articolul 5)*. Noul instrument juridic ar trebui să fie cât mai exact în ceea ce privește elementele esențiale care stabilesc legalitatea prelucrării datelor. Articolul 5 din directivă (precum și considerentul 9 al acesteia), care împuternicește statele membre să precizeze condițiile în care operațiunile de prelucrare sunt legale, poate, astfel, să nu mai fie necesar într-un viitor cadru juridic.

56. *Temeiul prelucrării datelor* (articolele 7 și 8). Definirea condițiilor în care are loc prelucrarea datelor constituie un element esențial al oricărei legislații privind protecția datelor. Statelor membre nu ar trebui să le fie permisă introducerea de motive suplimentare pentru prelucrarea datelor sau modificarea ori excluderea de motive. Posibilitatea acordării de derogări ar trebui exclusă sau limitată (în special în ceea ce privește datele sensibile ([30])). Într-un nou instrument juridic, temeiul prelucrării datelor ar trebui să fie clar formulat, reducând, astfel, libertatea de apreciere în momentul transpunerii sau aplicării noului instrument. În mod special, este posibil ca noțiunea de consimțământ să trebuiască a fi specificată mai exact (a se vedea secțiunea 6.5). De asemenea, temeiul privind interesul legitim urmărit de operator [articolul 7 litera (f)] lasă loc unor interpretări foarte diferite, dat fiind caracterul flexibil al acestui interes. Sunt necesare precizări suplimentare. O altă dispoziție care s-ar putea să trebuiască a fi clarificată este cuprinsă la articolul 8 alineatul (2) litera (b), care permite prelucrarea datelor sensibile în scopul respectării obligațiilor și drepturilor specifice ale operatorului în materie de drept al muncii ([31]).

57. *Drepturile persoanelor vizate* (articolele 10-15). Acesta este unul dintre domeniile în care nu toate elementele din directivă au fost implementate și interpretate în mod coerent de statele membre. Drepturile persoanelor vizate constituie un element central pentru o protecție eficientă a datelor. În consecință, spațiul de manevră ar trebui redus substanțial. AEPD recomandă ca informațiile furnizate de operator persoanelor vizate să fie uniforme la nivelul UE.

58. *Transferurile internaționale* (articolele 25-26). Acesta este un domeniu care a provocat critici ample din cauza lipsei unei practici uniforme la nivelul UE. Părțile interesate au criticat faptul că deciziile Comisiei privind nivelul adecvat de protecție sunt interpretate și puse în aplicare în moduri foarte diferite de statele membre. Regulile corporatiste obligatorii (*Binding Corporate Rules*, BCR) reprezintă un alt element pentru care AEPD recomandă o mai bună armonizare (a se vedea capitolul 9).

59. *Autoritățile naționale pentru protecția datelor* (articolul 28). Autoritățile naționale pentru protecția datelor se supun unor norme foarte divergente în cele 27 de state membre, în special în ceea ce privește statutul, resursele și competențele lor. Articolul 28 a contribuit parțial la această divergență din cauza lipsei de precizie ([32]), fiind necesară explicarea mai detaliată a acestuia, în conformitate cu Hotărârea Curții Europene de Justiție în cauza C-518/07 ([33]) (a se vedea, în continuare, capitolul 10).

5.4. *Simplificarea sistemului de notificare*

60. Cerințele de notificare (articolele 18-21 din Directiva 95/46/CE) reprezintă un alt domeniu în care statele membre s-au bucurat de libertate considerabilă. În Comunicare se recunoaște în mod just că un sistem armonizat ar reduce costurile și sarcina administrativă pentru operatorii de date ([34]).

61. Acesta este un domeniu în care simplificarea ar trebui să fie principalul obiectiv. Revizuirea cadrului în materie de protecție a datelor constituie o ocazie unică de a simplifica și/sau reduce în continuare domeniul cerințelor actuale de notificare. În Comunicare se recunoaște existența unui consens general la nivelul părților interesate potrivit căruia actualul sistem de notificare este destul de greoi și nu aduce, în sine, nicio valoare adăugată în ceea ce privește protecția datelor cu caracter personal ale persoanelor ([35]). Astfel, AEPD salută angajamentul Comisiei de a căuta diferite posibilități de simplificare ale actualului sistem de notificare.

62. În opinia AEPD, punctul de plecare al acestei simplificări ar fi trecerea de la un sistem în care notificarea reprezintă regula, cu excepția unor prevederi contrare (de exemplu, „sistemul scutirii"), la un sistem mai bine orientat. Sistemul scutirii s-a dovedit a fi ineficient, fiind pus în aplicare în mod incoerent în statele membre ([36]). AEPD propune analizarea următoarelor alternative:

([29]) A se vedea Avizul nr. 1/2010 al GL 29 privind conceptele de „operator" și de „persoană împuternicită de către operator" (GL 169).

([30]) Articolul 8 alineatele (4) și (5) autorizează, în prezent, statele membre să acorde, în anumite condiții, derogări suplimentare în ceea ce privește datele sensibile.

([31]) A se vedea, în acest sens, primul raport al Comisiei referitor la punerea în aplicare a Directivei privind protecția datelor, menționată anterior, p. 14.

([32]) Documentul Grupului de lucru privind viitorul vieții private, punctul 87.

([33]) Cauza C-518/07, *Comisia/Germania*, nepublicată încă în Culegere.

([34]) A se vedea nota de subsol nr. 26.

([35]) A se vedea nota de subsol nr. 26.

([36]) Raportul Grupului de lucru instituit în temeiul articolului 29 privind obligația de a notifica autoritățile de supraveghere naționale, cea mai bună utilizare a excepțiilor și simplificărilor și rolul responsabililor cu protecția datelor în Uniunea Europeană, GL 106, 2005, p. 7.

— limitarea obligației de notificare la tipuri specifice de operațiuni de prelucrare care presupun riscuri specifice (aceste notificări ar putea determina măsuri suplimentare precum verificarea prealabilă a prelucrării);

— simpla obligație de înregistrare impusă operatorilor de date (contrar înregistrării extinse a tuturor operațiunilor de prelucrare a datelor).

În plus, ar putea fi introdus un formular de notificare standard paneuropean, pentru a asigura abordări armonizate în ceea ce privește informațiile solicitate.

63. Revizuirea actualului sistem de notificare nu ar trebui să aducă atingere îmbunătățirii obligațiilor de verificare prealabilă în cazul anumitor obligații de prelucrare ce pot prezenta riscuri specifice (cum ar fi sistemele de informații la scară mare). AEPD ar agrea includerea în noul instrument juridic a unei liste neexhaustive de cazuri în care este necesară o astfel de verificare prealabilă. În acest scop, Regulamentul (CE) nr. 45/2001 privind protecția persoanelor fizice cu privire la prelucrarea datelor cu caracter personal de către instituțiile și organele comunitare oferă un model util ([37]).

5.5. *Un regulament, nu o directivă*

64. În sfârșit, AEPD apreciază că procesul de revizuire constituie, de asemenea, ocazia de a reconsidera tipul de instrument juridic pentru protecția datelor. Un regulament, un instrument unic aplicabil în mod direct în statele membre, reprezintă mijlocul cel mai eficient de apărare a dreptului fundamental la protecția datelor și de creare a unei piețe interne veritabile în care datele cu caracter personal să circule liber, iar nivelul de protecție să fie egal și independent de țara sau de sectorul în care sunt prelucrate datele.

65. Un regulament ar reduce posibilitatea interpretărilor contradictorii și diferențele nejustificate în transpunerea și aplicarea legii. De asemenea, ar reduce importanța stabilirii legii aplicabile operațiunilor de prelucrare în cadrul UE, care reprezintă unul dintre aspectele cele mai controversate ale sistemului actual (a se vedea capitolul 9).

66. În domeniul protecției datelor, un regulament este cu atât mai justificat, deoarece:

— articolul 16 din TFUE promovează, la nivelul tratatului, dreptul la protecția datelor cu caracter personal și prevede sau chiar impune un nivel uniform de protecție a persoanei fizice în UE;

— prelucrarea datelor are loc într-un mediu electronic în care frontierele interne dintre statele membre au devenit mai puțin relevante.

67. Alegerea unui regulament ca instrument general permite, atunci când este necesar, formularea unor dispoziții care se adresează în mod direct statelor membre în care este nevoie de flexibilitate. De asemenea, regulamentul nu afectează competența statelor membre de a adopta, dacă este cazul, norme suplimentare pentru protecția datelor, în conformitate cu legislația UE.

6. **Consolidarea drepturilor persoanelor fizice**

6.1. *Necesitatea consolidării drepturilor*

68. AEPD sprijină în totalitate propunerea prezentată în Comunicare de consolidare a drepturilor persoanelor fizice, întrucât instrumentele juridice existente nu oferă protecția deplină și eficientă necesară într-o societate digitalizată tot mai complexă.

69. Pe de o parte, dezvoltarea unei societăți digitalizate atrage o creștere netă a colectării, utilizării și transferului ulterior de date cu caracter personal într-un mod extrem de complex și netransparent. De multe ori persoanele nu cunosc sau nu înțeleg cum se întâmplă acest lucru, nici cine le colectează datele și nici cum să își exercite controlul. Un exemplu legat de acest fenomen este monitorizarea de către furnizorii de rețele de publicitate a activităților de navigare pe internet a persoanelor folosind module cookie sau alte dispozitive similare în scopul transmiterii de mesaje publicitare orientate. Atunci când vizitează site-urile web, utilizatorii nu se așteaptă la faptul că o parte terță invizibilă înregistrează aceste vizite și creează profiluri de utilizatori, pe baza informațiilor care reflectă stilul lor de viață sau ce anume le place sau nu.

70. Pe de altă parte, dezvoltarea stimulează partajarea proactivă de informații cu caracter personal de către persoanele fizice, de exemplu, în rețelele de socializare. Din ce în ce mai frecvent, tinerii fac parte dintr-o rețea de socializare și interacționează cu persoane de vârsta lor. Nu se cunoaște exact dacă persoanele (tinere) își dau seama de amploarea divulgării informațiilor și efectele pe termen lung ale acțiunilor lor.

6.2. *Creșterea transparenței*

71. Transparența este extrem de importantă în orice regim de protecție a datelor, nu numai datorită valorii sale inerente, ci și din cauză că permite exercitarea altor principii privind protecția datelor. Numai dacă au cunoștință de prelucrarea datelor, persoanele își vor putea exercita drepturile.

72. Mai multe dispoziții ale Directivei 95/46/CE fac referire la transparență. Articolele 10 și 11 prevăd obligația de informare a persoanelor fizice cu privire la colectarea datele lor cu caracter personal. În plus, articolul 12 recunoaște dreptul persoanelor de a primi o copie a propriilor date cu caracter personal, într-o formă inteligibilă (dreptul de acces). Articolul 15 recunoaște dreptul de acces la logica potrivit căreia sunt luate deciziile automatizate ce produc efecte juridice. Nu în ultimul rând, articolul 6 alineatul (1) litera (a), care prevede ca prelucrarea să fie corectă, include și o cerință de transparență. Datele cu caracter personal nu pot fi prelucrate din motive ascunse sau secrete.

([37]) A se vedea articolul 27 din regulament (JO L 8, 12.1.2001, p. 1).

73. Comunicarea propune adăugarea unui principiu general al transparenței. Ca reacție la această propunere, AEPD subliniază faptul că noțiunea de transparență este deja integrată în actualul cadru juridic privind protecția datelor, deși în mod implicit. Acest lucru se poate deduce din diferitele dispoziții referitoare la transparență, astfel cum s-a menționat la alineatul anterior. În opinia AEPD, includerea unui principiu *explicit* al transparenței ar putea adăuga valoare, indiferent dacă este sau nu legat de dispoziția existentă referitoare la prelucrarea corectă. Acest principiu ar spori securitatea juridică și ar confirma, de asemenea, faptul că un operator trebuie să prelucreze în orice situații datele cu caracter personal în mod transparent, nu doar la cerere sau atunci când este obligat în virtutea unei dispoziții legislative specifice.

74. Cu toate acestea, este probabil mai important să se consolideze dispozițiile legislative existente referitoare la transparență, de exemplu, ale articolelor 10 și 11 din Directiva 95/46/CE. Aceste dispoziții specifică elementele informațiilor care trebuie furnizate, însă nu precizează modalitățile. Mai exact, AEPD propune consolidarea dispozițiilor existente, prin:

— cerința privind furnizarea, de către operator, a unor informații privind prelucrarea datelor într-un mod ușor de accesat și ușor de înțeles și într-un limbaj simplu și clar ([38]). Informațiile respective trebuie să fie clare, vizibile și elocvente. Dispoziția ar putea cuprinde, de asemenea, obligația de a asigura înțelegerea facilă a informațiilor. Această obligație ar face ca politicile de confidențialitate opace sau dificil de înțeles să devină ilegale;

— cerința de furnizare facilă și directă a informațiilor către persoanele vizate. De asemenea, informațiile ar trebui să fie disponibile permanent și nu să dispară din mediul electronic după un timp foarte scurt. Acest lucru va ajuta utilizatorii să stocheze și să reproducă informațiile în viitor, accesul fiind în continuare permis.

6.3. *Sprijin pentru obligația de raportare a încălcării securității*

75. AEPD sprijină introducerea în instrumentul general a unei dispoziții referitoare la notificarea privind încălcarea datelor cu caracter personal, care extinde obligația inclusă deja în Directiva ePrivacy revizuită ca anumiți furnizori să notifice toți operatorii de date, astfel cum se propune în Comunicare. În Directiva ePrivacy revizuită, obligația se aplică exclusiv furnizorilor de servicii de comunicații electronice [furnizori de servicii de telefonie (inclusiv VoIP) și de acces la internet]. Această obligație nu se referă la alți operatori de date. Motivele care justifică obligația se aplică în totalitate operatorilor de date alții decât furnizorii de servicii de comunicații electronice.

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

76. Notificarea încălcării securității servește diferite scopuri. Cel mai evident, subliniat în Comunicare, este acela de a servi drept instrument de informare pentru a face cunoscute persoanelor fizice riscurile la care se expun atunci când datele lor cu caracter personal sunt compromise. Acest instrument le poate ajuta să ia măsurile necesare de reducere a unor asemenea riscuri. De exemplu, atunci când sunt alertate cu privire la încălcări care le afectează informațiile financiare, persoanele vor putea, printre altele, să își schimbe parolele sau să își anuleze conturile. În plus, notificarea încălcării securității contribuie la aplicarea eficace a altor principii și obligații cuprinse în directivă. De exemplu, cerințele privind notificarea încălcării securității stimulează operatorii de date să pună în aplicare măsuri de securitate mai puternice pentru a preveni încălcările. De asemenea, notificarea încălcării securității reprezintă un instrument de întărire a responsabilității operatorilor de date și, mai ales, de sporire a asumării răspunderii (a se vedea capitolul 7). În sfârșit, notificarea încălcării securității servește drept instrument pentru aplicarea normelor de către autoritățile pentru protecția datelor. Notificarea autorităților pentru protecția datelor cu privire la o încălcare poate conduce la o anchetă privind practicile generale ale unui operator de date.

77. Normele specifice privind încălcarea securității din Directiva ePrivacy, astfel cum a fost modificată, au fost dezbătute pe larg în etapa parlamentară a cadrului legislativ, anterior adoptării Directivei ePrivacy. În această dezbatere au fost luate în considerare avizele Grupului de lucru instituit în temeiul articolului 29 și ale AEPD, precum și opiniile părților interesate. Normele reflectă opiniile diferitelor părți interesate. Ele reprezintă un echilibru de interese: deși criteriile care stau la baza obligației de notificare sunt, în principiu, adecvate pentru protecția persoanelor, ele nu impun cerințe prea dificile și inutile.

6.4. *Consolidarea consimțământului*

78. Articolul 7 din Directiva privind protecția datelor menționează șase temeiuri juridice pentru prelucrarea datelor cu caracter personal. Consimțământul persoanei este unul dintre acestea. Unui operator de date îi este permisă prelucrarea datelor cu caracter personal în măsura în care persoanele și-au dat consimțământul informat ca datele lor să fie colectate și ulterior prelucrate.

79. În practică, utilizatorii au adesea un control limitat asupra propriilor date, în special în mediile tehnologice. Una dintre metodele utilizate uneori este consimțământul implicit, adică un consimțământ care a fost dedus. Acest consimțământ poate fi dedus dintr-o acțiune a persoanei (de exemplu, acțiunea constând în utilizarea unui site internet se consideră a reprezenta consimțământul ca datele utilizatorului să fie înregistrate în scopuri comerciale). De asemenea, consimțământul poate fi

dedus din tăcerea sau lipsa de acțiune a persoanei (debifarea unei rubrici bifate se consideră consimțământ).

80. Potrivit directivei, pentru ca un consimțământ să fie valabil, acesta trebuie să fie informat, liber acordat și specific. Consimțământul trebuie să reprezinte o indicare informată a dorințelor persoanei prin care aceasta își exprimă acordul cu privire la prelucrarea datelor sale cu caracter personal. Mijlocul prin care este acordat consimțământul trebuie să fie neechivoc.

81. Consimțământul care a fost dedus dintr-o acțiune și, în special, din tăcerea sau lipsa de acțiune este adesea un consimțământ echivoc. Totuși, nu este întotdeauna clar în ce anume constă un consimțământ real și neechivoc. Unii operatori de date exploatează această incertitudine, utilizând metode neadecvate pentru acordarea unui consimțământ real și neechivoc.

82. În lumina considerentelor de mai sus, AEPD susține poziția Comisiei referitoare la necesitatea clarificării limitelor de consimțământ și asigurării faptului că numai consimțământul foarte explicit clarificat este considerat consimțământ propriu-zis. În acest context, AEPD propune următoarele ([39]):

— ar putea fi luate în considerare mai multe situații în care să fie necesară exprimarea consimțământului explicit, în prezent, acestea fiind limitate la datele sensibile;

— adoptarea unor norme suplimentare privind consimțământul în mediul on-line;

— adoptarea unor norme suplimentare privind consimțământul în ceea ce privește prelucrarea datelor în scopuri secundare (de exemplu, prelucrarea este secundară prelucrării principale sau nu este evidentă);

— într-un instrument legislativ suplimentar, adoptat sau nu de Comisie în temeiul articolului 290 din TFUE, stabilirea tipului de consimțământ necesar, de exemplu, pentru a specifica nivelul de consimțământ cu privire la prelucrarea datelor de pe etichetele RFID ale produselor de consum sau la alte tehnici specifice.

6.5. *Portabilitatea datelor și dreptul de a fi uitat*

83. Portabilitatea datelor și dreptul de a fi uitat reprezintă două concepte corelate, prezentate în Comunicare, în scopul consolidării drepturilor persoanelor vizate. Aceste concepte sunt complementare principiilor menționate deja în directivă, prevăzând dreptul persoanei vizate de a respinge prelucrarea ulterioară a datelor sale personale, precum și obligația operatorului de date de a șterge informațiile imediat ce acestea nu mai sunt necesare scopului prelucrării.

84. Aceste două noțiuni au adăugat, în mare parte, valoare în contextul unei societăți informaționale, în care un număr din ce în ce mai mare de date sunt stocate în mod automatizat și păstrate pentru perioade de timp nedeterminate. Practica arată că, deși datele sunt încărcate de însăși persoana vizată, gradul de control pe care acesta îl are asupra propriilor date personale este practic foarte limitat. Aceasta cu atât mai mult cu cât memoria pe care o reprezintă internetul astăzi gigantică. În plus, dintr-o perspectivă economică, pentru un operator de date este mai costisitor să șteargă datele decât să le păstreze stocate. Prin urmare, exercitarea drepturilor persoanei contrazice tendința economică normală.

85. Atât portabilitatea datelor, cât și dreptul de a fi uitat ar putea contribui la o reechilibrare a balanței în favoarea persoanei vizate. Obiectivul privind portabilitatea datelor ar fi acela de a asigura un mai mare control al persoanei asupra propriilor informații, iar dreptul de a fi uitat ar asigura faptul că informațiile dispar automat după o anumită perioadă de timp, chiar dacă persoana vizată nu ia nicio măsură sau nu cunoaște faptul că datele au fost vreodată stocate.

86. Mai precis, portabilitatea datelor este înțeleasă ca posibilitatea utilizatorilor de a-și modifica preferințele cu privire la prelucrarea datelor lor, legate, în special, de noile servicii tehnologice. Din ce în ce mai mult, acesta este cazul serviciilor ce implică stocarea informațiilor, inclusiv a datelor cu caracter personal, cum ar fi telefonia mobilă, precum și al serviciilor care stochează fotografii, mesaje electronice și alte informații, uneori utilizând servicii de „cloud computing”.

87. Persoanele fizice trebuie să aibă posibilitatea de a schimba furnizorul, în mod facil și liber, și de a-și transfera datele lor personale la alt furnizor de servicii. AEPD consideră că drepturile existente stabilite în Directiva 95/46/CE ar putea fi consolidate prin includerea unui drept de portabilitate, în special în contextul serviciilor societății informaționale, pentru a sprijini persoanele fizice, asigurând permiterea accesului la informațiile lor personale de către furnizori și alți operatori relevanți și că, în același timp, foștii furnizori sau alți operatori șterg aceste informații, chiar dacă ar dori să le păstreze în propriile lor scopuri legitime.

88. Un „drept de a fi uitat” recent codificat ar asigura ștergerea datelor cu caracter personal sau interzicerea ca acestea să mai fie utilizate, fără a fi necesară vreo acțiune din partea persoanei vizate, însă cu condiția ca aceste date să fi fost deja stocate pe o anumită perioadă de timp. Cu alte

([39]) Grupul de lucru instituit în temeiul articolului 29 lucrează, în prezent, la un aviz referitor la „consimțământ”. Acest aviz ar putea conduce la propuneri suplimentare.

cuvinte, datelor li se va atribui un fel de dată a expirării. Acest principiu este deja afirmat în cauze soluționate de instanțele naționale sau aplicat în anumite sectoare specifice, de exemplu, pentru dosare de poliție, cazier sau dosare disciplinare: în unele legislații naționale, informațiile referitoare la persoane sunt șterse în mod automat sau urmează să nu mai fie utilizate ori diseminate după o perioadă de timp stabilită, fără a fi necesară o analiză prealabilă de la caz la caz.

89. În acest sens, noul „drept de a fi uitat" ar trebui corelat cu portabilitatea datelor. Valoarea adăugată care s-ar crea astfel este aceea că nu vor fi necesare eforturi sau insistențe din partea persoanei vizate pentru ca aceste date să fie șterse, deoarece acest lucru ar trebui să se întâmple într-un mod obiectiv și automat. Numai în situații foarte speciale, în care s-ar putea stabili necesitatea păstrării datelor pentru o perioadă mai lungă de timp, un operator de date ar putea fi îndreptățit să păstreze datele. Acest „drept de a fi uitat" ar inversa astfel sarcina probei de la persoana fizică la operatorul de date și ar constitui o setare de „confidențialitate" prestabilită pentru prelucrarea datelor cu caracter personal.

90. AEPD consideră că dreptul de a fi uitat s-ar putea dovedi util în special în contextul serviciilor societății informaționale. O obligație de ștergere sau de încetare a diseminării informațiilor după o perioadă de timp determinată este justificată în special în presă sau pe internet și cu precădere în rețelele de socializare. De asemenea, această obligație ar fi utilă în ceea ce privește echipamentele terminale: datele stocate pe dispozitive mobile sau pe computer ar fi șterse sau blocate automat, după o perioadă de timp determinată, când ele nu se mai află în posesia persoanei fizice. În acest sens, dreptul de a fi uitat poate fi transpus într-o obligație de „confidențialitate prin concept".

91. Pe scurt, opinia AEPD este că portabilitatea datelor și dreptul de a fi uitat sunt concepte utile și ar merita să fie incluse în instrumentul juridic, însă limitate probabil la mediul electronic.

6.6. *Prelucrarea datelor cu caracter personal referitoare la copii*

92. Directiva 95/46/CE nu prevede norme speciale referitoare la prelucrarea datelor cu caracter personal ale copiilor. Această directivă nu recunoaște necesitatea unei protecții speciale a copiilor în circumstanțe specifice, din cauza vulnerabilității lor, precum și din cauza insecurității juridice pe care o generează în special în următoarele domenii:

— colectarea datelor copiilor și modul în care aceștia trebuie informați cu privire la această colectare;

— modul în care se obține consimțământul copiilor. Întrucât nu există norme specifice privind modul de obținere a consimțământului copiilor și vârsta până la care persoanele ar trebui să fie considerate copii, aceste teme sunt tratate în temeiul legislației naționale, care diferă de la un stat membru la altul ([40]);

— modalitatea și condițiile în care copiii sau reprezentanții lor legali își pot exercita drepturile, în conformitate cu dispozițiile directivei.

93. AEPD consideră că interesele particulare ale copiilor ar fi mai bine protejate dacă noul instrument juridic ar conține dispoziții suplimentare care să se refere în mod special la colectarea și prelucrarea ulterioară a datelor copiilor. De asemenea, aceste dispoziții specifice ar oferi securitate juridică în acest domeniu specific și ar fi în avantajul operatorilor de date care, în prezent, sunt expuși diferitelor obligații legale.

94. AEPD propune includerea în instrumentul juridic a următoarelor dispoziții:

— o cerință de informare care să fie adaptată pentru copii, în măsura în care acest lucru ar facilita înțelegerea de către copii a ceea ce înseamnă colectarea datelor lor;

— alte cerințe de informare adaptate pentru copii privind modul în care informațiile trebuie furnizate și, dacă este posibil, privind conținutul acestora;

— o dispoziție specifică privind protejarea copiilor împotriva publicității comportamentale;

— principiul limitării scopului ar trebui consolidat în ceea ce privește datele referitoare la copii;

— unele categorii de date nu ar trebui niciodată colectate de la copii;

— un prag de vârstă. Sub acest prag, în general, informațiile ar trebui colectate numai cu acordul explicit și verificabil al părinților;

— dacă este necesar acordul părinților, ar trebui să se stabilească norme cu privire la modalitatea de autentificare a vârstei copilului, cu alte cuvinte, de a

([40]) Consimțământul este, de obicei, legat de vârstă atunci când copiii își pot asuma obligații contractuale. Aceasta este vârsta la care se presupune că au atins un anumit nivel de maturitate. De exemplu, legislația spaniolă prevede acordul parental pentru colectarea datelor referitoare la copii care nu au împlinit vârsta de 14 ani. Peste această vârstă, se consideră că aceștia sunt în măsură să își dea consimțământul. În Regatul Unit, legea privind protecția datelor nu face referire la o anumită vârstă sau prag de vârstă. Cu toate acestea, autoritatea pentru protecția datelor din această țară a interpretat că peste vârsta de 12 ani copiii își pot da consimțământul. În schimb, copiii sub 12 ani nu își pot da consimțământul și pentru a obține datele lor cu caracter personal este mai întâi necesar să se obțină permisiunea unui părinte sau a unui tutore.

cunoaște dacă un copil este minor și de a verifica acordul părinților. Acesta este un domeniu în care UE se poate inspira din modelele altor țări, de exemplu, Statele Unite ([41]).

6.7. *Mecanisme de recurs colectiv*

95. Consolidarea fondului drepturilor persoanelor fizice ar fi inutilă în lipsa unor mecanisme procedurale eficiente de executare a acestor drepturi. În acest context, AEPD recomandă introducerea în legislația UE de mecanisme de recurs colectiv pentru încălcarea normelor privind protecția datelor. În mod special, mecanismele de recurs colectiv care autorizează grupuri de cetățeni să își asocieze pretențiile într-o singură acțiune civilă ar putea constitui un instrument foarte puternic de facilitare a aplicării normelor privind protecția datelor ([42]). Această inovație este, de asemenea, sprijinită de autoritățile pentru protecția datelor în documentul Grupului de lucru privind viitorul vieții private.

96. În cazul în care impactul este mai mic, este puțin probabil ca victimele unei încălcări a normelor privind protecția datelor să determine introducerea de acțiuni individuale împotriva operatorilor, date fiind costurile, întârzierile, incertitudinile, riscurile și sarcinile la care ar fi expuse. Aceste dificultăți ar putea fi depășite sau simplificate substanțial dacă ar fi instituit un sistem de recurs colectiv, prin care victimele încălcării să fie autorizate să își asocieze pretențiile individuale într-o singură acțiune. De asemenea, AEPD ar agrea autorizarea unor entități competente, cum ar fi asociațiile consumatorilor sau organismele publice, pentru a introduce acțiuni în despăgubire în numele victimelor încălcărilor protecției datelor. Aceste acțiuni nu ar trebui să aducă atingere dreptului persoanei vizate de a introduce acțiuni individuale.

97. Acțiunile colective nu sunt importante numai pentru asigurarea despăgubirii integrale sau a altor măsuri corective, ci au, în mod indirect, un rol sporit de descurajare. Riscul de a antrena daune colective mari în aceste acțiuni ar înmulți stimulentele operatorilor pentru respectarea în mod eficient a normelor. În acest sens, o mai bună aplicare a legii la nivel privat, prin intermediul mecanismelor de recurs colectiv, ar completa aplicarea acesteia la nivel public.

98. Comunicarea nu exprimă o poziție cu privire la acest subiect. AEPD are cunoștință de dezbaterea care se desfășoară la nivel european cu privire la introducerea recursului colectiv pentru consumatori. De asemenea, AEPD cunoaște riscul exceselor pe care aceste mecanisme le pot crea, pe baza experienței din alte sisteme juridice. Totuși, acești factori nu constituie, în opinia AEPD, argumente suficiente pentru a respinge sau a amâna introducerea lor în legislația privind protecția datelor, având în vedere avantajele pe care le pot determina ([43]).

7. **Consolidarea rolului organizațiilor/operatorilor**

7.1. *Aspecte generale*

99. În opinia AEPD, pe lângă consolidarea drepturilor persoanelor fizice, un instrument juridic modern pentru protecția datelor trebuie să conțină mijloacele necesare care sporesc responsabilitatea operatorilor de date. Mai precis, cadrul juridic trebuie să conțină stimulente pentru operatorii de date din sectorul privat sau public care să includă, în mod proactiv, măsuri de protecție a datelor în procesele lor operaționale. În primul rând, aceste mijloace ar fi utile deoarece, așa cum s-a afirmat anterior, dezvoltările tehnologice au avut ca rezultat o creștere netă a colectării, utilizării și transferului ulterior de date cu caracter personal, ceea ce sporește riscurile pentru persoanele fizice în ceea ce privește confidențialitatea și protecția datelor lor cu caracter personal, riscuri care ar trebui compensate într-un mod eficient. În al doilea rând, cadrul juridic actual nu conține astfel de mijloace, cu câteva excepții de dispoziții bine definite (a se vedea mai jos), iar operatorii de date pot adopta o abordare *reactivă* a protecției datelor și a confidențialității și acționa doar după apariția unei probleme. Această abordare este reflectată în statisticile care arată că practicile de conformitate deficitare și pierderile de date reprezintă probleme recurente.

100. Potrivit AEPD, cadrul juridic actual nu este suficient pentru a asigura protecția eficace a datelor cu caracter personal nici în condițiile actuale, nici în viitor. Cu cât riscurile sunt mai mari, cu atât și necesitatea aplicării unor măsuri concrete care protejează informațiile la un nivel practic și asigură o protecție eficientă va fi mai mare. Dacă aceste măsuri proactive nu sunt puse în aplicare *de facto*, probabil erorile, accidentele și neglijențele vor continua, punând în pericol viața privată a persoanelor fizice în această societate din ce în ce mai digitalizată. Pentru aceasta, AEPD propune următoarele măsuri.

7.2. *Consolidarea responsabilității operatorilor de date*

101. AEPD recomandă introducerea în instrumentul juridic a unei noi dispoziții, prin care operatorii de date să fie obligați să pună în aplicare măsuri adecvate și eficace pentru a aplica principiile și obligațiile instrumentului juridic și a demonstra, la cerere, acest lucru.

([41]) În Statele Unite ale Americii, COPPA obligă operatorii de site-uri internet comerciale sau de servicii on-line adresate copiilor sub 13 ani să obțină acordul părinților înainte de colectarea informațiilor personale, iar pe operatorii de site-uri internet comerciale adresate publicului larg să fie conștienți de faptul că anumiți vizitatori sunt minori.

([42]) A se vedea, de asemenea, Avizul AEPD din 25 iulie 2007 privind Comunicarea Comisiei către Parlamentul European și Consiliu cu privire la continuarea programului de lucru pentru o mai bună punere în aplicare a Directivei privind protecția datelor (JO C 255, 27.10.2007, p. 10).

([43]) Unele legislații naționale conțin deja prevederi referitoare la instituirea unor mecanisme similare.

102. Acest tip de dispoziție nu este cu totul nou. Articolul 6 alineatul (2) din Directiva 95/46/CE face referire la principiile legate de calitatea datelor și menționează că „asigurarea respectării dispozițiilor alineatului (1) incumbă operatorului". De asemenea, articolul 17 alineatul (1) obligă operatorii de date să pună în aplicare măsuri tehnice și organizaționale. Cu toate acestea, domeniul de aplicare a acestor dispoziții este limitat. Introducerea unei dispoziții generale referitoare la responsabilitate ar stimula operatorii să instituie măsuri proactive pentru a putea respecta toate elementele legislației privind protecția datelor.

103. O dispoziție referitoare la responsabilitate ar avea drept consecință impunerea unei obligații asupra operatorilor de date de a institui mecanisme interne și sisteme de control pentru asigurarea respectării principiilor și obligațiilor cuprinse în cadrul juridic. Această dispoziție ar impune, de exemplu, implicarea conducerii de vârf în politicile de protecție a datelor, cartografierea de proceduri pentru asigurarea identificării corespunzătoare a tuturor operațiunilor de prelucrare a datelor, instituirea unor politici obligatorii de protecție a datelor care să fie, de asemenea, revizuite și actualizate permanent pentru a cuprinde noi operațiuni de prelucrare a datelor, respectarea principiilor privind calitatea datelor, avizarea, securitatea, accesul etc. De asemenea, dispoziția respectivă ar obliga operatorii să țină evidențe pentru a putea demonstra, la cererea autorităților, conformitatea. În anumite cazuri, demonstrarea conformității înaintea publicului larg ar trebui să fie obligatorie. Acest lucru s-ar putea realiza, de exemplu, prin impunerea obligației operatorilor de a include protecția datelor în rapoartele publice (anuale), atunci când aceste rapoarte sunt obligatorii din alte motive.

104. În mod evident, tipurile de măsuri interne și externe care vor fi puse în aplicare trebuie să fie adecvate și să depindă de faptele și circumstanțele specifice fiecărui caz în parte. Există o mare diferență între un operator care prelucrează câteva sute de dosare de clienți, constând doar în nume și adrese, și un altul care prelucrează dosarele a milioane de pacienți, care includ antecedentele medicale ale acestora. Același lucru este valabil și pentru modalitățile specifice în care trebuie evaluată eficacitatea măsurilor. Este necesară proporționalitatea.

105. Instrumentul juridic general global pentru protecția datelor nu ar trebui să stabilească cerințele specifice de responsabilitate, ci numai elementele esențiale ale acesteia. Comunicarea prevede anumite elemente de întărire a responsabilității operatorilor de date, care sunt bine-venite. Mai precis, AEPD sprijină pe deplin obligativitatea evaluării responsabililor cu protecția datelor și a impactului asupra confidențialității, în anumite condiții-limită.

106. În plus, AEPD recomandă delegarea competențelor către Comisie, în temeiul articolului 290 din TFUE, pentru a completa cerințele de bază necesare îndeplinirii standardului de responsabilitate. Utilizarea acestor competențe va spori securitatea juridică a operatorilor de date și va armoniza conformitatea în UE. La elaborarea acestor instrumente specifice ar trebui consultate Grupul de lucru instituit în temeiul articolului 29, precum și AEPD.

107. În sfârșit, măsurile concrete legate de responsabilitate, care vor fi puse în aplicare de operatorii de date ar putea fi, de asemenea, impuse de autoritățile pentru protecția datelor, în contextul competențelor lor de aplicare a legii. Pentru aceasta, ar trebui să se atribuie noi competențe autorităților pentru protecția datelor, care să le permită să impună măsuri corective sau sancțiuni. Exemplele ar trebui să includă stabilirea unor programe de conformitate interne pentru implementarea confidențialității prin concept în produse și servicii specifice etc. Măsurile corective ar trebui impuse în măsura în care sunt adecvate, proporționate și eficiente pentru asigurarea conformității cu standardele legale aplicabile.

7.3. Confidențialitatea prin concept

108. Confidențialitatea prin concept se referă la integrarea protecției datelor și a vieții private chiar din momentul conceperii noilor produse, servicii și proceduri care implică prelucrarea de date cu caracter personal. În opinia AEPD, confidențialitatea prin concept reprezintă un element de responsabilitate. În consecință, operatorii de date vor fi obligați să demonstreze că au pus în aplicare și confidențialitatea prin concept atunci când a fost necesar. Recent, cu ocazia celei de a 32-a Conferințe internaționale a comisarilor pentru protecția datelor și a vieții private, a fost emisă o rezoluție prin care confidențialitatea prin concept este recunoscută ca o componentă esențială a protecției dreptului fundamental la viață privată ([44]).

109. Directiva 95/46/CE conține o serie de dispoziții care încurajează confidențialitatea prin concept ([45]), însă nu recunoaște în mod explicit această obligație. AEPD se declară mulțumită de faptul că, în Comunicare, confidențialitatea prin concept este acceptată ca mijloc de asigurare a conformității cu normele privind protecția datelor. AEPD propune includerea unei dispoziții obligatorii care să stabilească obligația „confidențialității prin concept", care s-ar putea baza pe considerentul 46 din Directiva 95/46/CE. Mai precis, dispoziția ar impune operatorilor de date, în mod explicit, obligația de a pune în aplicare măsuri tehnice și organizatorice, atât în momentul proiectării sistemului de prelucrare, cât și în cel al prelucrării în

([44]) Rezoluția privind confidențialitatea prin concept, adoptată de cea de a 32-a Conferință internațională a comisarilor pentru protecția datelor și a vieții private, Ierusalim, 27-29 octombrie 2010.

([45]) Directiva include dispoziții care, în mod indirect și în diferite situații, impun implementarea confidențialității prin concept. În mod special, articolul 17 prevede obligația operatorilor de date de a pune în aplicare măsuri tehnice și organizatorice adecvate pentru a împiedica prelucrarea ilegală a datelor. Directiva ePrivacy este mai explicită. Articolul 14 alineatul (3) prevede că „dacă este necesar, se pot adopta măsuri care să asigure că echipamentele terminale sunt construite într-un mod care să le facă compatibile cu dreptul utilizatorilor de a proteja și de a controla folosirea datelor lor personale, în conformitate cu Directiva 1999/5/CE și cu Decizia 87/95/CEE a Consiliului din 22 decembrie 1986 privind standardizarea în domeniul tehnologiei informațiilor și al comunicațiilor".

sine, în special în scopul asigurării protecției datelor cu caracter personal și prevenirii oricărei prelucrări neautorizate ([46]).

110. În baza unei asemenea dispoziții, operatorii de date ar fi obligați, printre altele, să se asigure că sistemele de prelucrare a datelor sunt concepute să prelucreze cât mai puține date cu caracter personal, să includă setări de confidențialitate prestabilite, de exemplu, în rețelele de socializare, pentru a păstra confidențialitatea prestabilită a profilurilor persoanelor fizice și să utilizeze mijloace care să permită utilizatorilor să își protejeze mai bine datele lor personale (de exemplu, controlul accesului, criptarea).

111. Avantajele unei trimiteri mai explicite la confidențialitatea prin concept pot fi sintetizate după cum urmează:

— ar sublinia importanța principiului în sine, ca mijloc de asigurare a faptului că procesele, produsele și serviciile sunt concepute ținând seama, de la început, de confidențialitate;

— ar reduce abuzurile asupra vieții private și ar reduce la minimum colectarea inutilă de date, oferind persoanelor posibilitatea de a opera o alegere reală în privința datelor lor personale;

— ar evita necesitatea unor „bandaje" ulterioare, în încercarea de a rezolva probleme care pot fi dificil de remediat, dacă nu chiar imposibil;

— de asemenea, ar facilita aplicarea efectivă a acestui principiu de către autoritățile pentru protecția datelor.

112. Efectul combinat al acestei obligații ar avea ca rezultat o cerere mai mare de produse și servicii ce asigură confidențialitatea prin concept, ceea ce ar trebui să stimuleze mai mult industria în satisfacerea acestei cereri. În plus, ar trebui avută în vedere crearea unei obligații separate pentru proiectanții și producătorii de noi produse și servicii cu posibil impact asupra protecției datelor și a vieții private. AEPD propune includerea unei asemenea obligații separate care ar putea permite operatorilor de date să respecte într-o mai mare măsură propria obligație.

113. Codificarea confidențialității prin concept ar putea fi completată de o dispoziție care să stabilească cerințele generale privind confidențialitatea prin concept, aplicabile tuturor sectoarelor, produselor și serviciilor, cum ar fi, de exemplu, asigurarea unor măsuri de autorizare a utilizatorului, care să fie adoptate conform principiului respectiv.

114. În plus, AEPD recomandă delegarea competențelor către Comisie, în temeiul articolului 290 din TFUE, pentru a suplimenta, dacă este cazul, cerințele de bază privind confidențialitatea prin concept pentru produsele și serviciile selectate. Utilizarea acestor competențe ar spori securitatea juridică a operatorilor de date și ar armoniza conformitatea la nivelul întregii UE. La elaborarea acestor instrumente specifice, ar trebui consultate Grupul de lucru instituit în temeiul articolului 29, precum și AEPD (a se vedea, de asemenea, punctul 106 referitor la responsabilitate).

115. În sfârșit, autorităților pentru protecția datelor ar trebui să le fie atribuită competența de a impune măsuri corective sau sancțiuni, în condiții restrictive similare celor deja menționate la punctul 107, în cazul în care operatorii nu iau măsuri concrete atunci când acest lucru ar fi necesar.

7.4. *Servicii de certificare*

116. În Comunicare se recunoaște necesitatea de a analiza crearea de scheme de certificare UE pentru produsele și serviciile conforme cu cerințele privind confidențialitatea. AEPD sprijină pe deplin acest obiectiv și propune includerea unei dispoziții privind crearea acestor scheme și posibilele efecte în UE, care poate fi dezvoltată ulterior într-o dispoziție legislativă suplimentară. Dispoziția respectivă ar trebui să completeze prevederile referitoare la responsabilitate și confidențialitate prin concept.

117. Schemele de certificare voluntară ar crea posibilitatea de a verifica dacă un operator de date a instituit măsuri în scopul conformării cu prevederile instrumentului juridic. În plus, există posibilitatea ca operatorii de date sau chiar produsele și serviciile care dețin o etichetă de certificare să obțină un avantaj concurențial față de alții. Aceste scheme ar ajuta, de asemenea, autoritățile pentru protecția datelor în îndeplinirea rolului lor de supraveghere și de aplicare a legii.

8. **Globalizarea și legislația aplicabilă**

8.1. *O nevoie clară de protecție mai consecventă*

118. Astfel cum s-a menționat în capitolul 2, transferul datelor cu caracter personal în afara frontierelor UE a crescut exponențial ca urmare a dezvoltării noilor tehnologii, a rolului companiilor multinaționale și a influenței sporite a guvernelor în prelucrarea și efectuarea de schimburi de date cu caracter personal la scară internațională. Acesta este unul dintre principalele motive care justifică revizuirea actualului cadru juridic și, prin urmare, unul dintre domeniile în care AEPD face apel la ambiție și eficacitate, întrucât există o nevoie clară de protecție mai consecventă atunci când datele sunt prelucrate în afara UE.

([46]) În cadrul juridic actual, considerentul 46 încurajează operatorii să pună în aplicare astfel de măsuri, însă un considerent nu are, desigur, caracter obligatoriu.

8.2. *Investiții în norme internaționale*

119. În opinia AEPD, sunt necesare mai multe investiții în elaborarea de norme internaționale. Mai buna armonizare în ceea ce privește nivelul de protecție a datelor cu caracter personal în lume ar clarifica mult mai bine conținutul principiilor care trebuie respectate, precum și condițiile de efectuare a transferului de date. Aceste norme globale ar trebui să armonizeze cerința referitoare la un standard ridicat de protecție a datelor, inclusiv elementele esențiale ale protecției datelor în UE, și caracteristicile regionale.

120. AEPD sprijină eforturile ambițioase depuse până acum în cadrul Conferinței internaționale a comisarilor pentru protecția datelor și a vieții private de a elabora și disemina așa-numitele „standarde de la Madrid", în vederea integrării lor într-un instrument obligatoriu și, posibil, în vederea inițierii unei conferințe interguvernamentale ([47]). AEPD invită Comisia să ia inițiativele necesare pentru a facilita realizarea acestui obiectiv.

121. De asemenea, AEPD consideră că este important să se asigure consecvența între această inițiativă de elaborare a unor standarde internaționale, actuala revizuire a cadrului juridic european privind protecția datelor și alte evoluții precum revizuirea actuală a Orientărilor OCDE privind viața privată și a Convenției nr. 108 a Consiliului Europei care este deschisă pentru semnare de țările terțe (a se vedea, de asemenea, punctul 17). În opinia AEPD, Comisia are de jucat un rol specific în acest sens, trebuind să explice cum va promova această coerență în negocierile din cadrul OCDE și al Consiliului Europei.

8.3. *Clarificarea criteriilor de drept aplicabile*

122. Întrucât consecvența totală nu poate fi ușor de obținut, cel puțin în viitorul apropiat, va persista o oarecare diferență între legislațiile din interiorul UE și, cu siguranță, cele de dincolo de frontierele acesteia. AEPD consideră că noul instrument juridic va trebui să clarifice criteriile de determinare a legislației aplicabile și să asigure mecanisme modernizate de control al fluxului de date, precum și responsabilitatea actorilor implicați în realizarea fluxurilor de date.

123. În primul rând, instrumentul juridic ar trebui să asigure faptul că legislația UE este aplicabilă atunci când datele cu caracter personal sunt prelucrate în afara frontierelor UE, dar numai în cazul în care există o solicitare justificată de aplicare a legislației UE. Exemplul serviciilor de „cloud computing" neeuropene vizând rezidenți ai UE este o ilustrare a motivului pentru care acest lucru este necesar. Într-un mediu în care datele nu sunt stocate fizic și prelucrate într-o locație determinată în care furnizorii de servicii și utilizatorii din diferite țări exercită o influență perturbatoare asupra datelor, este foarte dificil de identificat cine este responsabil pentru respectarea căror principii privind protecția datelor. Sunt oferite orientări, în special de către autoritățile pentru protecția datelor, cu privire la interpretarea și aplicarea Directivei 95/46/CE în astfel de cazuri, însă orientările nu sunt suficiente pentru a asigura securitatea juridică în acest mediu nou.

124. Într-un aviz recent ([48]), Grupul de lucru instituit în temeiul articolului 29 a subliniat necesitatea unui cadru juridic mai exact și a unui criteriu simplificat de determinare a legislației aplicabile pe teritoriul UE.

125. Potrivit AEPD, opțiunea preferată ar fi instituirea unui instrument juridic sub forma unui regulament care să conducă la norme identice aplicabile în toate statele membre. Un regulament ar face ca necesitatea determinării legislației aplicabile să fie mai puțin importantă. Acesta este unul dintre motivele pentru care AEPD pledează în favoarea adoptării unui regulament. Cu toate acestea, un regulament ar putea lăsa o marjă de manevră statelor membre. În cazul în care în noul instrument se va menține o oarecare marjă de manevră, AEPD va sprijini propunerea Grupului de lucru privind trecerea de la o aplicare distributivă a diferitelor legislații naționale la o aplicare centralizată a unei legislații unice în toate statele membre în care un operator are unități. De asemenea, AEPD pledează pentru o mai bună cooperare și coordonare între autoritățile pentru protecția datelor în cauzele și plângerile transnaționale (a se vedea capitolul 10).

8.4. *Raționalizarea mecanismelor de control al fluxului de date*

126. Necesitatea consecvenței și a unui nivel de referință ridicat trebuie luată în considerare nu doar din perspectiva principiilor globale privind protecția datelor, ci și în ceea ce privește transferurile internaționale. AEPD sprijină pe deplin obiectivul Comisiei de a raționaliza procedurile actuale privind transferul internațional de date și de a asigura o abordare mai uniformă și coerentă față de țările terțe și organizațiile internaționale.

127. Mecanismul fluxurilor de date include atât transferurile din sectorul privat, în special prin intermediul clauzelor contractuale sau al Regulilor corporatiste obligatorii, cât și transferurile între autoritățile publice. Regulile corporatiste obligatorii reprezintă unul dintre elementele pentru care ar fi de dorit o abordare mai coerentă și raționalizată. AEPD recomandă abordarea explicită a condițiilor pentru Regulile corporatiste obligatorii în noul instrument juridic ([49]), prin:

— recunoașterea explicită a Regulilor corporatiste obligatorii ca mijloace care oferă garanții adecvate;

— stabilirea elementelor/condițiilor principale pentru adoptarea Regulilor corporatiste obligatorii;

([47]) Astfel cum s-a propus prin Rezoluția privind standardele internaționale, adoptată la cea de a 32-a Conferință internațională a comisarilor pentru protecția datelor și a vieții private, Ierusalim, 27-29 octombrie 2010.

([48]) Avizul 8/2010 al Grupului de lucru instituit în temeiul articolului 29 privind legislația aplicabilă, GL 179.

([49]) Referitor la transferurile internaționale, a se vedea, de asemenea, capitolul 8 din prezentul aviz.

— stabilirea unor proceduri de cooperare pentru adoptarea Regulilor corporatiste obligatorii, inclusiv a criteriilor de selecție a unei autorități de supraveghere principale (ghișeu unic).

9. **Domeniile poliției și justiției**

9.1. *Instrumentul general*

128. Comisia a subliniat în mod repetat importanța consolidării protecției datelor în contextul aplicării legii și prevenirii infracționalității, în care schimbul și utilizarea de informații cu caracter personal s-a intensificat în mod semnificativ. De asemenea, Programul de la Stockholm, aprobat de Consiliul European, face referire la un regim solid de protecție a datelor ca principală condiție prealabilă a strategiei UE de gestionare a informațiilor în acest domeniu ([50]).

129. Revizuirea cadrului general privind protecția datelor constituie ocazia perfectă pentru a realiza progrese în acest sens, în special din moment ce Comunicarea descrie, în mod just, Decizia-cadru 2008/977 ca fiind inadecvată ([51]).

130. În secțiunea 3.2.5 din prezentul aviz, AEPD menționează motivele pentru care domeniul cooperării polițienești și judiciare ar trebui inclus în instrumentul general. Includerea poliției și justiției prezintă o serie de avantaje suplimentare. Acest lucru înseamnă că normele nu se vor mai aplica doar schimburilor transfrontaliere de date ([52]), ci și prelucrării datelor la nivel intern. Protecția adecvată în cadrul schimbului de date cu caracter personal cu țările terțe va fi garantată într-o mai mare măsură, inclusiv în ceea ce privește acordurile internaționale. În plus, autoritățile pentru protecția datelor vor avea aceleași competențe extinse și armonizate față de autoritățile polițienești și judiciare pe care le au și față de alți operatori de date. În sfârșit, actualul articol 13 care prevede competența statelor membre de a adopta legislația specifică de limitare a obligațiilor și drepturilor din cadrul instrumentului general, pentru interese publice specifice, va trebui să fie aplicat în același mod restrictiv în care se aplică în alte domenii. În mod special, garanțiile specifice prevăzute de instrumentul general în acest domeniu vor trebui respectate și în legislația națională adoptată în domeniul cooperării polițienești și judiciare.

9.2. *Norme suplimentare specifice domeniului poliției și justiției*

131. Totuși, această includere nu exclude normele și derogările speciale care țin seama, în mod corespunzător, de caracteristicile acestui sector, în conformitate cu Declarația nr. 21 anexată la Tratatul de la Lisabona. Pot fi prevăzute limitări ale drepturilor persoanelor vizate, însă cu condiția ca acestea să fie necesare, proporționate și să nu afecteze elementele esențiale ale dreptului propriu-zis. În acest context, ar trebui subliniat faptul că, în prezent, Directiva 95/46/CE, inclusiv articolul 13, este valabilă pentru aplicarea legii în diverse domenii (de exemplu, fiscal, vamal, antifraudă) care nu diferă în mod fundamental de multe activități din domeniul poliției și justiției.

132. În plus, trebuie instituite, de asemenea, garanții specifice pentru a compensa persoana vizată, oferindu-i protecție suplimentară într-un domeniu în care prelucrarea datelor cu caracter personal poate fi mai intruzivă.

133. În lumina celor de mai sus, AEPD consideră că noul cadru juridic ar trebui să includă cel puțin următoarele elemente, conform Convenției nr. 108 și Recomandării nr. R (87) 15:

— o distincție între diferitele categorii de date și dosare, în funcție de exactitatea și fiabilitatea acestora, aderând la principiul potrivit căruia ar trebui să se facă deosebire între datele bazate pe fapte și datele bazate pe opinii sau aprecieri personale;

— o distincție între diversele categorii de persoane vizate (presupuși infractori, victime, martori etc.) și de dosare (temporare, permanente și de informații confidențiale). Este necesar să se prevadă condiții și garanții specifice pentru prelucrarea datelor persoanelor care nu sunt suspectate;

— mecanisme prin care să se asigure verificarea și rectificarea periodică, pentru a garanta calitatea datelor care sunt prelucrate;

— dispozițiile și/sau garanțiile specifice pot fi elaborate în raport cu prelucrarea (din ce în ce mai relevantă) a datelor biometrice și genetice în domeniul aplicării legii. Utilizarea acestora ar trebui să se limiteze doar la cazurile în care nu sunt disponibile mijloace mai puțin intruzive care pot asigura aceleași efecte ([53]);

— condițiile de realizare a transferurilor de date cu caracter personal către autorități necompetente și persoane particulare, precum și condițiile de accesare și de utilizare ulterioară de către autoritățile de aplicare a legii a datelor cu caracter personal colectate de persoane particulare.

([50]) A se vedea, în acest sens, Avizul AEPD din 30 septembrie 2010 privind Comunicarea Comisiei către Parlamentul European și Consiliu – „Prezentare generală asupra modului de gestionare a informațiilor în spațiul de libertate, securitate și justiție", paragrafele 9-19.

([51]) A se vedea secțiunea 3.2.5 de mai sus.

([52]) În prezent, aceasta este sfera de aplicare limitată a Deciziei-cadru 2008/977.

([53]) În acest sens, a se vedea documentul GL privind viitorul vieții private, punctul 112.

9.3. *Sisteme de protecție a datelor de natură sectorială*

134. Comunicarea afirmă că „decizia-cadru nu înlocuiește diferitele instrumente legislative de natură sectorială care au fost adoptate la nivelul UE în domeniile cooperării polițienești și judiciare în materie penală, în special cele care reglementează funcționarea Europol, Eurojust, Sistemului de informații Schengen (SIS) și Sistemului de informații al vămilor (CIS), care fie prevăd regimuri speciale de protecție a datelor, fie se referă în general la instrumente de protecție a datelor ale Consiliului Europei".

135. În opinia AEPD, un nou cadru juridic ar trebui, pe cât posibil, să fie clar, simplu și coerent. Dat fiind că există o proliferare a diferitelor regimuri aplicabile, de exemplu, Europol, Eurojust, SIS și Prüm, conformitatea cu normele rămâne sau devine chiar mai complicată. Acesta este unul dintre motivele pentru care AEPD pledează pentru un instrument juridic global pentru toate sectoarele.

136. AEPD înțelege însă faptul că alinierea normelor din diferite sisteme va necesita un volum considerabil de muncă ce trebuie desfășurată atent. AEPD consideră că o abordare graduală, astfel cum se menționează în Comunicare, este justificată atât timp cât angajamentul de asigurare a unui nivel ridicat de protecție a datelor într-un mod coerent și eficient rămâne clar și vizibil. Mai concret:

— într-o primă etapă, instrumentul juridic general pentru protecția datelor ar trebui să fie aplicabil tuturor prelucrărilor de date din domeniul cooperării polițienești și judiciare, inclusiv adaptărilor pentru poliție și justiție (astfel cum se menționează în secțiunea 9.2);

— într-o a doua etapă, regimurile de protecție a datelor de natură sectorială ar trebui aliniate la acest instrument general. Comisia ar trebui să se angajeze în adoptarea de propuneri pentru această a doua etapă, într-un termen de timp scurt, specificat.

10. **Autoritățile pentru protecția datelor (APD) și cooperarea dintre acestea**

10.1. *Consolidarea rolului APD*

137. AEPD sprijină pe deplin obiectivul Comisiei de soluționare a problemei statutului autorităților pentru protecția datelor și, mai precis, de consolidare a independenței, resurselor și competențelor acestora de aplicare a legii.

138. De asemenea, AEPD insistă asupra necesității ca noul instrument juridic să clarifice noțiunea de independență a APD. Curtea Europeană de Justiție a adoptat deja o decizie în acest sens în cauza C-518/07 ([54]), în care a subliniat faptul că independență înseamnă absența oricărei influențe externe. O autoritate pentru protecția datelor poate solicita să nu primească instrucțiuni de la nimeni. AEPD propune în mod explicit codificarea acestor elemente de independență în legislație.

139. Pentru îndeplinirea sarcinilor lor, APD trebuie să dispună de suficiente resurse umane și financiare. AEPD propune includerea acestei cerințe în legislație ([55]), evidențiind, în cele din urmă, necesitatea de a asigura că autoritățile dețin competențe complet armonizate în ceea ce privește investigarea și impunerea de măsuri de descurajare, corective și de sancțiuni. Acest lucru ar consolida securitatea juridică a persoanelor vizate și a operatorilor de date.

140. Consolidarea independenței, resurselor și competențelor autorităților pentru protecția datelor ar trebui combinată cu cooperarea consolidată la nivel multilateral, în special ținând seama de numărul tot mai mare de probleme legate de protecția datelor la nivel european. Principala infrastructură care urmează a fi utilizată pentru această cooperare este, în mod evident, Grupul de lucru instituit în temeiul articolului 29.

10.2. *Consolidarea rolului Grupului de lucru*

141. Experiența arată că, de la înființarea în 1997 și până în prezent, funcționarea Grupului de lucru a evoluat. Acesta s-a îndreptat spre o mai mare independență, nemaiputând fi considerat practic un simplu grup de lucru consultativ al Comisiei. AEPD propune îmbunătățirea în continuare a funcționării Grupului de lucru, inclusiv a infrastructurii și independenței acestuia.

142. AEPD consideră că soliditatea Grupului de lucru este legată în mod intrinsec de independența și competența membrilor săi. Autonomia Grupului de lucru ar trebui să fie asigurată în noul cadru juridic, conform criteriilor stabilite de Curtea Europeană de Justiție în cauza C-518/07 în ceea ce privește independența totală a autorităților pentru protecția datelor. De asemenea, AEPD consideră că Grupului de lucru ar trebui să i se asigure suficiente resurse și buget, precum și un secretariat consolidat, pentru a sprijini eforturile acestuia.

143. În ceea ce privește secretariatul Grupului de lucru, AEPD apreciază faptul că acesta este integrat în unitatea pentru protecția datelor a DG Justiție, cu avantajul că Grupul de lucru propriu-zis poate beneficia de contacte eficiente și flexibile și de informații la zi privind evoluțiile din domeniul protecției datelor. Pe de altă parte, AEPD ridică semne de întrebare cu privire la calitatea Comisiei (mai precis a unității) de membru, secretariat și, totodată, de destinatar al avizelor Grupului de lucru. Acest lucru ar justifica o mai mare independență a secretariatului. AEPD încurajează Comisia să evalueze, consultând îndeaproape părțile interesate, modul în care această independență poate fi cel mai bine asigurată.

([54]) Cauza C-518/07, *Comisia/Germania*, nepublicată încă în Culegere.

([55]) A se vedea, de exemplu, articolul 43 alineatul (2) din Regulamentul (CE) nr. 45/2001, care prevede această cerință pentru AEPD.

144. În sfârșit, consolidarea competențelor APD necesită, de asemenea, competențe mai mari ale Grupului de lucru, cu o structură care să includă norme și garanții mai bune, precum și mai multă transparență. Această structură va fi dezvoltată atât pentru rolul consultativ al Grupului, cât și pentru rolul său de aplicare a legii.

10.3. *Rolul consultativ al Grupului de lucru*

145. Pozițiile exprimate de Grupul de lucru trebuie implementate efectiv atunci când vine vorba de rolul consultativ al acestuia pentru Comisie, în special în legătură cu interpretarea și aplicarea principiilor directivei și alte instrumente de protecție a datelor, cu alte cuvinte pentru a asigura caracterul oficial al pozițiilor exprimate de Grupul de lucru. Sunt necesare dezbateri suplimentare în rândul APD pentru a identifica modul în care această cerință poate fi inclusă în instrumentul juridic.

146. AEPD recomandă soluții care vor spori autoritatea avizelor grupului de lucru, fără a modifica substanțial modul de funcționare a acestuia. AEPD propune includerea obligației autorităților pentru protecția datelor și a Comisiei de a ține seama cu strictețe de avizele și pozițiile comune adoptate de Grupul de lucru, pe baza modelului adoptat pentru pozițiile exprimate de Organismul autorităților europene de reglementare în domeniul comunicațiilor electronice (OAREC) ([56]). Mai mult decât atât, noul instrument juridic ar putea atribui Grupului de lucru sarcina explicită de a adopta „recomandări interpretative". Aceste soluții alternative ar conferi un rol mai important pozițiilor exprimate de Grupul de lucru, inclusiv înaintea instanțelor.

10.4. *Aplicarea coordonată a legii de către Grupul de lucru*

147. În cadrul juridic actual, aplicarea legislației privind protecția datelor în statele membre este de competența autorităților pentru protecția datelor din cele 27 de state membre, cu un nivel redus de coordonare în ceea ce privește gestionarea cazurilor specifice. În ceea ce privește cazurile în care sunt implicate mai multe state membre sau care au, în mod clar, o dimensiune globală, costurile pentru întreprinderi se multiplică, acestea fiind obligate să se adreseze mai multor autorități publice diferite pentru aceeași activitate, iar riscurile aplicării incoerente cresc: în cazuri excepționale, aceleași activități de prelucrare pot fi considerate legale de o autoritate pentru protecția datelor și interzise de o alta.

148. Unele cazuri au o dimensiune strategică ce ar trebui abordată într-o manieră centralizată. Grupul de lucru instituit în temeiul articolului 29 facilitează coordonarea și măsurile de aplicare sau executorii între APD ([57]), în probleme majore legate de protecția datelor cu implicații internaționale. Acesta a fost cazul rețelelor sociale și motoarelor de căutare ([58]), precum și al verificărilor coordonate efectuate în diferite state membre cu privire la telecomunicații și asigurări de sănătate.

149. Există însă limite pentru măsurile de aplicare pe care Grupul de lucru și le poate asuma în cadrul juridic actual. Grupul de lucru poate adopta poziții comune, dar nu există niciun instrument pentru asigurarea punerii efective în practică a acestora.

150. AEPD propune includerea în instrumentul juridic a unor dispoziții suplimentare care ar putea sprijini aplicarea coordonată, în special a următoarelor:

— obligația APD și a Comisiei de a ține seama cu strictețe de avizele și pozițiile comune adoptate de GL 29 ([59]);

— obligația APD de a coopera loial una cu cealaltă și cu Comisia și GL 29 ([60]). Ca exemplu practic al unei cooperări loiale, ar putea fi stabilită o procedură prin care APD să informeze Comisia sau Grupul de lucru în cazul măsurilor de aplicare naționale ce conțin un element transfrontalier, prin analogie cu procedura aplicabilă în cadrul juridic actual în ceea ce privește deciziile naționale privind nivelul adecvat de protecție;

— specificarea regulilor de vot pentru sporirea angajamentului APD de a pune în aplicare deciziile Grupului de lucru. Ar putea fi introdusă o dispoziție care să oblige Grupul de lucru să vizeze adoptarea deciziilor pe baza consensului, iar atunci când nu se poate ajunge la un consens, acesta să adopte aplicarea

([56]) Regulamentul (CE) nr. 1211/2009 al Parlamentului European și al Consiliului din 25 noiembrie 2009 de instituire a Organismului autorităților europene de reglementare în domeniul comunicațiilor electronice (OAREC) și a Oficiului (JO L 337, 18.12.2009, p. 1).

([57]) În afara Grupului de lucru instituit în temeiul articolului 29, Conferința europeană a comisarilor pentru protecția datelor a creat, cu aproape 10 ani în urmă, un atelier permanent cu scopul de a trata într-o manieră coordonată plângerile transfrontaliere. Cu toate că prezintă o valoare adăugată incontestabilă în ceea ce privește schimburile dintre personalul APD, oferind o rețea fiabilă de puncte de contact, acest atelier nu poate fi considerat drept mecanism de coordonare a procesului decizional.

([58]) A se vedea scrisorile GL 29 din 12 mai 2010 și 26 mai 2010, publicate pe site-ul internet al GL 29 (http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/2010-others_en.htm).

([59]) Astfel cum s-a menționat anterior, Regulamentul (CE) nr. 1211/2009 stabilește o obligație similară prin care se specifică rolul Organismului autorităților europene de reglementare în domeniul comunicațiilor electronice (OAREC).

([60]) A se vedea, în acest sens, articolul 3 din Regulamentul (CE) nr. 1211/2009, menționat anterior.

doar cu o majoritate calificată. În plus, s-ar putea introduce un considerent care să prevadă că autoritățile pentru protecția datelor care acordă un vot pozitiv referitor la un document, să aibă obligația sau să își asume angajamentul politic de a pune în aplicare, la nivel național, dispozițiile respectivului document.

151. AEPD și-ar exprima rezerva față de introducerea unor măsuri mai stricte, cum ar fi atribuirea unui caracter obligatoriu pozițiilor GL 29. Acest lucru ar submina statutul independent al autorităților pentru protecția datelor, care trebuie garantat de statele membre în temeiul legislației naționale. În cazul în care deciziile Grupului de lucru ar avea un impact direct asupra părților terțe precum operatorii de date, ar trebui să fie prevăzute proceduri noi care să includă garanții cum ar fi transparența și căile de atac, inclusiv probabil, introducerea de recursuri pe lângă Curtea Europeană de Justiție.

10.5. *Cooperarea dintre AEPD și Grupul de lucru*

152. De asemenea, ar putea fi îmbunătățită cooperarea între AEPD și Grupul de lucru. AEPD este membru al Grupului de lucru, în cadrul căruia participă la pozițiile adoptate asupra principalelor evoluții strategice ale UE, asigurând, totodată, compatibilitatea cu propriile poziții. AEPD remarcă numărul tot mai mare de probleme legate de viața privată, atât în sectorul privat, cât și în cel public, având implicații la nivel național în multe state membre, în soluționarea cărora este necesar ca Grupul de lucru să joace un rol specific.

153. AEPD are sarcina suplimentară de a oferi consultanță în ceea ce privește evoluțiile în contextul UE, care ar trebui menținută. În calitate de organism european, AEPD își exercită această competență consultativă față de instituțiile UE în același mod în care APD naționale oferă consultanță guvernelor lor.

154. AEPD și Grupul de lucru acționează dintr-o perspectivă diferită, dar complementară. Din aceste motive, este necesară menținerea și poate chiar îmbunătățirea coordonării între Grupul de lucru și AEPD pentru a asigura colaborarea acestora în ceea ce privește principalele aspecte privind protecția datelor, de exemplu, prin coordonarea periodică a agendelor ([61]) și asigurarea transparenței asupra problemelor care au un caracter mai național sau specific Uniunii Europene.

155. Directiva actuală nu menționează coordonarea din simplul motiv că AEPD nu exista la momentul adoptării acesteia, însă după șase ani de existență a AEPD, complementaritatea AEPD și a Grupului de lucru este vizibilă și ar putea fi recunoscută oficial. AEPD amintește faptul că, în conformitate cu Regulamentul (CE) nr. 45/2001, are sarcina de a coopera cu APD naționale și de a lua parte la activitățile Grupului de lucru. AEPD recomandă menționarea în mod explicit a cooperării în noul instrument juridic, precum și structurarea acesteia atunci când este necesar, de exemplu, prin instituirea unei proceduri de cooperare.

10.6. *Cooperarea dintre AEPD și APD în ceea ce privește supravegherea sistemelor UE*

156. Aceste considerente se aplică și în domeniile în care supravegherea trebuie coordonată între nivelul european și cel național. Acest lucru este valabil în cazul organismelor UE care prelucrează volume considerabile de date furnizate de autoritățile naționale sau în cazul sistemelor de informații la scară mare având o componentă europeană și una națională.

157. Pentru unele organisme UE și sisteme de informații la scară mare, de exemplu, Europol, Eurojust și prima generație a Sistemului de informații Schengen (SIS) care au organe de control comune, cu reprezentanți ai APD naționale, sistemul actual reprezintă o rămășiță a cooperării interguvernamentale din perioada anterioară Tratatului de la Lisabona care nu respectă structura instituțională a UE, din care Europol și Eurojust fac în prezent parte integrantă și în care a fost acum integrat și „acquis-ul Schengen" ([62]).

158. Comunicarea anunță lansarea în 2011 de către Comisie a unei consultări a părților interesate cu privire la revizuirea acestor sisteme de control. AEPD îndeamnă Comisia să adopte, cât mai curând posibil (într-un interval de timp scurt, specificat – a se vedea mai sus) o poziție în cadrul dezbaterilor actuale privind controlul, în care AEPD va avea următorul punct de vedere.

159. Încă de la început, ar trebui garantat faptul că toate organele de control îndeplinesc criteriile indispensabile privind independența, resursele și competențele de aplicare a legii. Mai mult, ar trebui să se asigure că sunt luate în considerare perspectivele și expertiza existente la nivelul UE. Acest lucru înseamnă că ar trebui să existe cooperare nu numai între autoritățile naționale, ci și cu autoritatea europeană pentru protecția datelor (AEPD) care consideră necesar să se respecte un model care îndeplinește aceste cerințe ([63]).

160. În ultimii ani, a fost dezvoltat modelul de „supraveghere coordonată". Acest model de supraveghere, așa cum funcționează în prezent în Eurodac și parțial în Sistemul de informații al vămilor, va fi extins în curând la Sistemul de informații privind vizele (VIS) și la a doua generație a Sistemului de informații Schengen (SIS II). Acest model are trei niveluri: 1. controlul la nivel național este

([61]) De exemplu, pe baza inventarului legislativ publicat anual și actualizat periodic, disponibil pe site-ul internet al AEPD.

([62]) În temeiul Regulamentului (CE) nr. 45/2001, AEPD are obligația de a coopera cu aceste organisme.

([63]) Pentru Eurojust, modelul ar trebui să țină seama și de faptul că supravegherea protecției datelor respectă independența justiției, în măsura în care Eurojust prelucrează date în contextul procedurilor penale.

asigurat de APD; 2. controlul la nivelul UE este asigurat de AEPD; 3. coordonarea este asigurată prin intermediul reuniunilor periodice convocate de AEPD acționând în calitate de secretariat al acestui mecanism de coordonare. Acest model s-a dovedit a fi reușit și eficient și ar trebui prevăzut, în viitor, pentru alte sisteme de informații.

C. **CUM SE POATE ÎMBUNĂTĂȚI APLICAREA ACTUALULUI CADRU JURIDIC?**

11. **Pe termen scurt**

161. Cu toate că procesul de revizuire este în desfășurare, ar trebui depuse eforturi pentru asigurarea aplicării complete și efective a normelor actuale. Aceste norme vor fi încă valabile până la adoptarea viitorului cadru juridic și transpunerea sa ulterioară în legislațiile naționale ale statelor membre. În acest sens, se pot identifica mai multe direcții de acțiune.

162. În primul rând, Comisia ar trebui să continue monitorizarea respectării Directivei 95/46/CE de către statele membre și, atunci când este necesar, să facă uz de competențele care îi revin în temeiul articolului 258 din TFUE. Recent, au fost lansate proceduri de încălcare a dreptului comunitar pentru aplicarea incorectă a articolului 28 din Directivă privind cerința referitoare la independența APD ([64]). De asemenea, deplina conformitate trebuie monitorizată și aplicată și în alte domenii ([65]). Astfel, AEPD salută și sprijină în totalitate angajamentul Comisiei menționat în Comunicare de a duce o politică activă de sancționare a încălcărilor dreptului comunitar. De asemenea, Comisia ar trebui să continue dialogul structural cu statele membre în ceea ce privește punerea în aplicare ([66]).

163. În al doilea rând, aplicarea legii la nivel național trebuie încurajată, astfel încât să se asigure aplicarea în practică a normelor privind protecția datelor, inclusiv în raport cu noile fenomene tehnologice și actorii globali. Autoritățile pentru protecția datelor ar trebui să facă uz de toate competențele în materie de investigare și sancționare. De asemenea, este important ca drepturile existente ale persoanelor vizate, în special dreptul de acces, să fie pe deplin aplicate în practică.

164. În al treilea rând, pe termen scurt se pare că este necesară o mai bună coordonare în aplicarea legii. În acest sens, rolul GL 29 și al documentelor interpretative ale acestuia este crucial, însă autoritățile pentru protecția datelor ar trebui, de asemenea, să depună toate eforturile pentru a le pune în practică. Soluționarea contradictorie a cauzelor la nivelul UE și la nivel internațional trebuie evitată, iar în cadrul Grupului de lucru este posibil și ar trebui să se ajungă la abordări comune. Anchetele coordonate la nivelul UE cu sprijinul Grupului de lucru pot crea, de asemenea, o importantă valoare adăugată.

165. În al patrulea rând, principiile privind protecția datelor ar trebui „integrate” proactiv în noi regulamente care pot avea un impact direct sau indirect asupra protecției datelor. La nivelul UE, AEPD depune eforturi considerabile pentru a contribui la îmbunătățirea legislației europene, iar aceste eforturi trebuie asumate și la nivel național. Autoritățile pentru protecția datelor ar trebui, așadar, să își utilizeze în totalitate competențele consultative pentru a asigura o astfel de abordare proactivă. Autoritățile pentru protecția datelor, inclusiv AEPD, pot juca, de asemenea, un rol proactiv în monitorizarea dezvoltărilor tehnologice. Monitorizarea este importantă în vederea identificării tendințelor emergente într-o etapă timpurie, evidențierii posibilelor implicații pentru protecția datelor, sprijinirii soluțiilor avantajoase în ceea ce privește protecția datelor și sensibilizării părților interesate.

166. În sfârșit, trebuie urmărită în mod activ o mai bună cooperare între diferiții actori la nivel internațional. Prin urmare, consolidarea instrumentelor de cooperare internațională este importantă, iar inițiative precum standardele de la Madrid și activitatea desfășurată în prezent în cadrul Consiliului Europei și al OCDE merită susținere totală. În acest context, este bine-venită intrarea Comisiei federale pentru comerț din SUA în familia comisarilor pentru protecția datelor și a vieții private în cadrul Conferinței internaționale a acestora.

D. **CONCLUZII**

OBSERVAȚII GENERALE

167. AEPD salută, în general, Comunicarea Comisiei, fiind convinsă că revizuirea actualului cadru juridic privind protecția datelor este necesară pentru a asigura o protecție eficace într-o societate informațională globalizată în continuă dezvoltare.

168. Comunicarea identifică principalele probleme și provocări. AEPD împărtășește punctul de vedere al Comisiei, potrivit căruia, în viitor, va fi, totuși, necesar un sistem solid de protecție a datelor, bazat pe ideea că principiile generale existente privind protecția datelor sunt încă valabile într-o societate care suferă schimbări fundamentale. AEPD este de acord cu afirmația din Comunicare referitoare la faptul că provocările sunt uriașe și subliniază consecința că soluțiile propuse ar trebui să fie pe măsură de ambițioase și să sporească eficacitatea protecției. Prin urmare, AEPD solicită o abordare mai ambițioasă a mai multor puncte.

169. AEPD sprijină pe deplin abordarea globală a protecției datelor. Cu toate acestea, regretă faptul că această Comunicare exclude din instrumentul juridic general anumite domenii, de exemplu, prelucrarea datelor de instituțiile și organismele UE. În cazul în care Comisia ar decide eliminarea acestor domenii, AEPD îndeamnă Comisia să

([64]) A se vedea cauza C-518/07, menționată anterior, și comunicatul de presă al Comisiei din 28 octombrie 2010 (IP/10/1430).

([65]) Comisia a inițiat o procedură de încălcare a dreptului comunitar împotriva Regatului Unit pentru o presupusă încălcare a mai multor dispoziții privind protecția datelor, inclusiv a cerinței privind confidențialitatea comunicațiilor electronice în ceea ce privește publicitatea comportamentală. A se vedea comunicatul de presă al Comisiei din 9 aprilie 2009 (IP/09/570).

([66]) A se vedea primul raport al Comisiei referitor la punerea în aplicare a Directivei privind protecția datelor, menționat anterior, p. 22 și următoarele.

adopte o propunere pentru nivelul UE în cel mai scurt termen posibil, de preferință, până la sfârșitul anului 2011.

PERSPECTIVE PRINCIPALE

170. În opinia AEPD, punctele de plecare ale procesului de revizuire sunt următoarele:

— măsurile de protecție a datelor trebuie, pe cât posibil, să sprijine, nu să împiedice alte interese legitime (cum ar fi economia europeană, securitatea persoanelor fizice și răspunderea guvernelor);

— principiile generale privind protecția datelor nu ar trebui și nu pot fi modificate;

— mai buna armonizare ar trebui să constituie unul dintre obiectivele esențiale ale revizuirii;

— perspectiva drepturilor fundamentale ar trebui să reprezinte punctul central al procesului de revizuire. Un drept fundamental vizează protecția cetățenilor în toate circumstanțele;

— noul instrument juridic trebuie să includă sectorul poliției și justiției;

— noul instrument juridic trebuie formulat pe cât posibil într-un mod neutru din punct de vedere tehnologic și trebuie să vizeze crearea unei securități juridice pe termen lung.

ELEMENTE ALE UNUI NOU CADRU

Armonizarea și simplificarea

171. AEPD salută angajamentul Comisiei de a analiza mijloacele de realizare a unei mai bune armonizări a protecției datelor la nivelul UE. AEPD stabilește domeniile în care mai buna organizare reprezintă o urgență: definițiile, temeiul prelucrării datelor, drepturile persoanelor vizate, transferurile internaționale și autoritățile pentru protecția datelor.

172. AEPD propune luarea în considerare a următoarelor alternative pentru simplificarea și/sau reducerea domeniului de aplicare a cerințelor de notificare:

— limitarea obligației de notificare la tipuri specifice de operațiuni de prelucrare care presupun riscuri specifice;

— obligația simplei înregistrări, care să impună operatorilor de date să înregistreze (contrar înregistrării extensive a tuturor operațiunilor de prelucrare a datelor);

— introducerea unui formular-standard de notificare paneuropean.

173. Potrivit AEPD, un regulament, un instrument unic direct aplicabil în statele membre, reprezintă mijlocul cel mai eficient de protejare a dreptului fundamental de protecție a datelor și de obținere a unei mai bune convergențe în cadrul pieței interne.

Consolidarea drepturilor persoanelor fizice

174. AEPD sprijină propunerea de consolidare a drepturilor persoanelor fizice prevăzută în Comunicare. AEPD propune următoarele:

— în legislație ar putea fi inclus un principiu al transparenței, însă este mai importantă consolidarea dispozițiilor existente referitoare la transparență (cum ar fi actualele articole 10 și 11 din Directiva 95/46/CE);

— în instrumentul general ar trebui introdusă o dispoziție privind notificarea încălcării datelor cu caracter personal, care să extindă obligația prevăzută de Directiva ePrivacy revizuită, de la anumiți furnizori la toți operatorii de date;

— limitele consimțământului ar trebui să fie clarificate. Ar trebui să se ia în considerare creșterea numărului de cazuri în care este necesar consimțământul expres, precum și adoptarea unor norme suplimentare pentru mediul on-line;

— ar trebui introduse drepturi suplimentare, cum ar fi portabilitatea datelor și dreptul de a fi uitat, în special pentru serviciile societății informaționale pe internet;

— interesele copiilor ar trebui să fie mai bine protejate printr-o serie de dispoziții suplimentare care să vizeze în mod specific la colectarea și prelucrarea ulterioară a datelor copiilor;

— în legislația UE ar trebui introduse mecanisme de recurs colectiv pentru încălcarea normelor privind protecția datelor, pentru a autoriza entitățile competente să introducă acțiuni în numele unor grupuri de persoane.

Întărirea obligațiilor organizațiilor/operatorilor

175. Noul cadru juridic trebuie să prevadă stimulente pentru operatorii de date pentru ca aceștia să includă, în mod proactiv, măsuri de protecție a datelor în procesele lor operaționale. AEPD propune introducerea unor dispoziții generale privind responsabilitatea și „confidențialitatea prin concept". De asemenea, ar trebui introdusă o dispoziție privind sistemele de certificare a confidențialității.

Globalizarea și legislația aplicabilă

176. AEPD sprijină eforturile ambițioase depuse în cadrul Conferinței internaționale a comisarilor pentru protecția datelor pentru elaborarea așa-numitelor „standarde de la Madrid" în vederea integrării acestora într-un instrument obligatoriu și probabil în vederea inițierii unei conferințe interguvernamentale. AEPD invită Comisia să ia măsuri concrete în această direcție, în strânsă cooperare cu OCDE și Consiliul Europei.

177. Noul instrument juridic trebuie să stabilească criteriile de determinare a legislației aplicabile. Ar trebui să se asigure faptul că datele care sunt prelucrate în afara frontierelor UE intră sub jurisdicția UE atunci când există un temei justificat de aplicare a dreptului UE. În cazul în care cadrul juridic ar lua forma unui regulament, ar exista norme identice în toate statele membre, iar determinarea legislației aplicabile (în cadrul UE) ar deveni mai puțin relevantă.

178. AEPD sprijină pe deplin obiectivul de a asigura o abordare mai uniformă și coerentă în ceea ce privește țările terțe și organizațiile internaționale. Regulile corporatiste obligatorii ar trebui incluse în instrumentul juridic.

Domeniile poliției și justiției

179. Un instrument cuprinzător care include poliția și justiția poate permite elaborarea unor norme speciale care să țină seama, în mod corespunzător, de caracteristicile acestui sector, conform Declarației nr. 21 anexate la Tratatul de la Lisabona. Este necesară instituirea unor garanții specifice pentru a compensa persoanele vizate, oferindule un nivel suplimentar de protecție într-un domeniu în care prelucrarea datelor cu caracter personal este, prin natura sa, mai intruzivă.

180. Noul cadru juridic ar trebui să fie cât mai clar, simplu și coerent. Ar trebui evitată proliferarea diferitelor regimuri aplicabile, de exemplu, pentru Europol, Eurojust, SIS și Prüm. AEPD înțelege că alinierea normelor diferitelor sisteme va trebui efectuată atent și în mod progresiv.

APD și cooperarea dintre acestea

181. AEPD sprijină pe deplin obiectivul Comisiei de a soluționa problema statutului APD și de a consolida independența, resursele și competențele acestora de aplicare a legii. AEPD recomandă următoarele:

— codificarea în noul instrument juridic a noțiunii esențiale de independență a APD, conform specificației Curții Europene de Justiție;

— prevederea în legislație a faptului că autoritățile pentru protecția datelor trebuie să dispună de resurse suficiente;

— atribuirea APD de competențe armonizate de anchetă și sancționare.

182. AEPD propune îmbunătățirea în continuare a funcționării Grupului de lucru instituit în temeiul articolului 29, inclusiv a independenței și infrastructurii acestuia. De asemenea, Grupului de lucru ar trebui să i se asigure suficiente resurse și un secretariat consolidat.

183. AEPD propune consolidarea rolului consultativ al Grupului de lucru, prin introducerea obligației APD și a Comisiei de *a ține seama cu strictețe de avizele și pozițiile comune* adoptate de Grupul de lucru. AEPD nu pledează pentru atribuirea unui caracter obligatoriu pozițiilor Grupului de lucru, în special datorită statutului independent al autorităților individuale pentru protecția datelor. AEPD recomandă ca în noul instrument juridic Comisia să introducă dispoziții specifice privind consolidarea cooperării cu AEPD.

184. AEPD invită Comisia să adopte în cel mai scurt timp o poziție față de problema supravegherii organismelor UE și a sistemelor de informații la scară mare, ținând seama de faptul că toate organismele de supraveghere ar trebui să îndeplinească criteriile indispensabile privind independența, resursele suficiente și competențele executorii și fiind asigurată o bună reprezentare a perspectivei UE. AEPD susține modelul „supravegherii coordonate”.

Îmbunătățiri în cadrul sistemului actual:

185. AEPD încurajează Comisia:

— să continue monitorizarea respectării dispozițiilor Directivei 95/46/CE de către statele membre și, atunci când este necesar, utilizarea competențelor executorii în temeiul articolul 258 din TFUE;

— să promoveze aplicarea legii la nivel național și coordonarea aplicării legii;

— să integreze în mod proactiv principiile privind protecția datelor în noile regulamente care pot avea un impact direct sau indirect asupra protecției datelor;

— să urmărească în mod activ cooperarea dintre diferiții actori la nivel internațional.

Adoptat la Bruxelles, 14 ianuarie 2011.

Peter HUSTINX

Autoritatea Europeană pentru Protecția Datelor