I

(Rezoluții, recomandări și avize)

AVIZE

AUTORITATEA EUROPEANĂ PENTRU PROTECȚIA DATELOR

Avizul Autorității Europene pentru Protecția Datelor privind Raportul final al Grupului de contact la nivel înalt UE-SUA privind schimbul de informații și protecția vieții private și a datelor cu caracter personal

(2009/C 128/01)

AUTORITATEA EUROPEANĂ PENTRU PROTECȚIA DATELOR,

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

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

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

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, în special articolul 41,

ADOPTĂ PREZENTUL AVIZ

I. INTRODUCERE – CONTEXTUL AVIZULUI

1. La 28 mai 2008, Președinția Consiliului Uniunii Europene a anunțat Coreper, în perspectiva summitului UE de la 12 iunie 2008, că Grupul de contact la nivel înalt UE-SUA (denumit în continuare „GCNÎ") privind schimbul de informații și protecția vieții private și a datelor cu caracter personal și-a finalizat raportul. Acest raport a fost făcut public la data de 26 iunie 2008 ([1]).

2. Raportul încearcă să identifice principii comune pentru protecția vieții private și a datelor cu caracter personal ca un prim pas către schimbul de informații cu Statele Unite în combaterea terorismului și a formelor grave de criminalitate transnațională.

3. În anunțul său, Președinția Consiliului afirmă că va saluta orice idei cu privire la acțiunile de întreprins în continuarea acestui raport, și în special reacții la recomandările privind căile de urmat identificate în raport. AEPD răspunde acestei invitații emițând următorul aviz, întemeiat pe situația actuală, astfel cum a fost făcută aceasta publică și fără a aduce atingere oricărei poziții ulterioare pe care ar putea să o adopte având în vedere evoluția chestiunii.

4. AEPD ia notă de faptul că activitatea GCNÎ s-a desfășurat într-un context care a asistat, cu precădere începând cu 11 septembrie 2001, la dezvoltarea schimbului de date între SUA și UE, prin acorduri internaționale sau alte tipuri de instrumente. Printre acestea se numără acordurile Europol și Eurojust cu Statele Unite, precum și acordurile privind registrele cu numele pasagerilor (PNR) și cazul Swift, care a generat un schimb de scrisori între autoritățile UE și autoritățile SUA pentru stabilirea unor garanții minime în materie de protecție a datelor ([2]).

([1]) Documentul Consiliului nr. 9831/08, disponibil la: http://ec.europa.eu/justice_home/fsj/privacy/news/index_en.htm

([2]) — Acordul între Statele Unite ale Americii și Oficiul European de Poliție din 6 decembrie 2001 și Acordul suplimentar între Europol și SUA privind schimbul de date cu caracter personal și de informații aferente, publicat pe site-ul web al Europol;
— Acordul între Statele Unite ale Americii și Eurojust privind cooperarea judiciară, 6 noiembrie 2006, publicat pe site-ul web al Eurojust;
— Acordul între Uniunea Europeană și Statele Unite ale Americii privind prelucrarea și transferul de date din registrul cu numele pasagerilor (PNR), de către transportatorii aerieni, către Departamentul pentru Securitate Internă al Statelor Unite (DHS) (Acordul PNR 2007), semnat la Bruxelles, la 23 iulie 2007 și la Washington, la 26 iulie 2007, JO L 204, 4.8.2007, p. 18;
— Schimb de scrisori între autoritățile SUA și autoritățile UE privind „Terrorist Finance Tracking Program" (Programul de urmărire a finanțării activităților teroriste), 28 iunie 2007.

5. Mai mult, UE negociază de asemenea și acceptă instrumente similare permițând schimbul de date cu caracter personal cu alte țări terțe. Un exemplu recent este constituit de Acordul între Uniunea Europeană și Australia privind prelucrarea și transferul datelor din registrul de nume al pasagerilor (PNR) provenind din Uniunea Europeană de către transportatorii aerieni către Serviciul vamal australian ([3]).

6. Reiese din acest context că solicitările autorităților de aplicare a legii din țările terțe cu privire la informații cu caracter personal devin în mod constant din ce în ce mai ample, și că acestea se extind, de asemenea, de la tradiționalele baze de date guvernamentale la alte tipuri de dosare, în special dosare cu date colectate de către sectorul privat.

7. Cu titlul de element contextual important, AEPD reamintește, de asemenea, faptul că chestiunea transferului de date cu caracter personal către țări terțe în cadrul cooperării polițienești și judiciare în materie penală este abordată în Decizia-cadru a Consiliului privind protecția datelor cu caracter personal prelucrate în cadrul cooperării polițienești și judiciare în materie penală ([4]), cu privire la care se preconizează că urmează să fie adoptată înainte de sfârșitul anului 2008.

8. Se preconizează că acest schimb transatlantic de informații poate evolua doar spre creștere și poate atinge sectoare colaterale în care sunt prelucrate date cu caracter personal. Într-un asemenea context, un dialog privind „aplicarea legii la nivel transatlantic" este în același timp salutar și delicat. Este salutar în sensul că ar putea furniza un cadru mai clar pentru schimburile de date aflate în curs de desfășurare sau care urmează să aibă loc. Este însă în egală măsură delicat, deoarece un asemenea cadru ar putea legitima transferuri de date masive într-un domeniu – aplicarea legii – în care impactul asupra persoanelor fizice este extrem de semnificativ și în care, cu atât mai mult, este nevoie de măsuri de securitate și garanții stricte și fiabile ([5]).

9. Prezentul aviz va aborda în capitolul următor situația actuală și posibilele căi de urmat. Capitolul III se va concentra pe domeniul de aplicare și natura unui instrument care ar permite schimbul de informații. În capitolul IV, avizul va analiza dintr-o perspectivă generală chestiuni juridice legate de conținutul unui posibil acord. Acesta va aborda chestiuni precum condițiile de evaluare a nivelului de protecție oferit în Statele Unite și va discuta chestiunea utilizării cadrului de reglementare al UE drept criteriu de referință pentru a evalua nivelul acestei protecții. Prezentul capitol va enumera, de asemenea, cerințele de bază care ar trebui să fie incluse într-un asemenea acord. În cele din urmă, în capitolul V avizul va prezenta o analiză a principiilor privind viața privată anexată raportului.

([3]) JO L 213, 8.8.2008, p. 49.

([4]) Decizia-cadru a Consiliului privind protecția datelor cu caracter personal prelucrate în cadrul cooperării polițienești și judiciare în materie penală, versiunea din 24 iunie 2008 disponibilă la http://ec.europa.eu/prelex/detail_dossier_real.cfm?CL=en&DosId=193371

([5]) Cu privire la necesitatea unui cadru juridic clar, a se vedea capitolele III și IV din prezentul aviz.

II. SITUAȚIA ACTUALĂ ȘI POSIBILELE CĂI DE URMAT

10. AEPD evaluează situația actuală după cum urmează. Au fost înregistrate unele progrese către definirea unor standarde comune privind schimbul de informații și protecția vieții private și a datelor cu caracter personal.

11. Cu toate acestea, lucrările pregătitoare pentru orice tip de acord între UE și SUA nu sunt încă finalizate. Sunt necesare eforturi suplimentare. Însuși raportul GCNÎ menționează un număr de chestiuni nesoluționate, printre care chestiunea „căilor de atac" este cea mai semnificativă. Dezacordul persistă cu privire la domeniul de aplicare necesar al căilor de atac ([6]). Alte cinci chestiuni nesoluționate au fost identificate în capitolul 3 al raportului. Mai mult, rezultă din prezentul aviz că multe alte chestiuni nu sunt încă soluționate, de exemplu în ceea ce privește domeniul de aplicare și natura unui instrument privind schimbul de informații.

12. Deoarece opțiunea preferată de raport este un acord cu forță juridică obligatorie – AEPD împărtășește această preferință – se impune cu atât mai mult o atitudine prudentă. Sunt necesare pregătiri suplimentare realizate cu atenție și în profunzime înainte de obținerea unui acord.

13. În ultimul rând, conform AEPD, încheierea unui acord ar trebuie să aibă loc la modul ideal sub Tratatul de la Lisabona, evident în funcție de intrarea în vigoare a acestuia. Într-adevăr, sub Tratatul de la Lisabona, nu ar exista nicio nesiguranță juridică cu privire la linia de demarcare între pilonii UE. Mai mult, implicarea deplină a Parlamentului European ar fi garantată, ca și controlul judiciar exercitat de Curtea de Justiție.

14. În aceste condiții, calea optimă de urmat ar consta în elaborarea unei foi de parcurs către un posibil acord la o etapă ulterioară. Această foaie de parcurs ar putea conține următoarele elemente:

— îndrumări pentru continuarea activității GCNÎ (sau a oricărui altui grup), precum și un termen;

— într-o etapă incipientă, discuții și un posibil acord asupra unor chestiuni fundamentale precum domeniul de aplicare și natura acordului;

— pe baza unei înțelegeri comune a acestor chestiuni fundamentale, elaborarea în continuare a principiilor în materie de protecție a datelor;

— implicarea părților interesate în diferite etape ale procedurii;

— în partea europeană, abordarea constrângerilor instituționale.

([6]) Pagina 5 a raportului, sub C.

III. DOMENIUL DE APLICARE ȘI NATURA UNUI INSTRUMENT PRIVIND SCHIMBUL DE INFORMAȚII

15. În opinia AEPD, este crucială definirea clară a domeniului de aplicare și a naturii unui posibil instrument incluzând principii privind protecția datelor, ca un prim pas pe calea elaborării ulterioare a unui asemenea instrument.

16. În ceea ce privește domeniul de aplicare, întrebări importante care trebuie să primească un răspuns sunt:

— cine sunt actorii implicați, din interiorul și din afara sferei aplicării legii;

— ce se intenționează prin „scopul aplicării legii", precum și relația dintre acesta și alte scopuri precum securitatea națională, și într-un mod mai specific controlul frontierelor și sănătatea publică;

— cum s-ar integra instrumentul în perspectiva unui spațiu global de securitate transatlantică.

17. Definiția naturii instrumentului ar trebui să clarifice următoarele chestiuni;

— în cazul în care este pertinent, în cadrul cărui pilon va fi negociat instrumentul;

— dacă instrumentul va avea forță juridică obligatorie pentru UE și SUA;

— dacă instrumentul va avea un efect direct, în sensul că conține drepturi și obligații pentru persoanele fizice a căror aplicare poate fi asigurată în fața unei autorități judiciare;

— dacă instrumentul în sine va permite schimbul de informații sau va stabili un standard minim pentru schimbul de informații, care să fie completat de acorduri specifice;

— în ce mod se va raporta instrumentul în cauză la instrumentele deja existente: le va respecta, le va înlocui sau le va completa?

III.1. Domeniul de aplicare al instrumentului

Actori implicați

18. Deși nu există nicio indicație clară în raportul GCNÎ cu privire la domeniul de aplicare precis al viitorului instrument, se poate deduce din principiile menționate în raport că acesta are în vedere acoperirea atât a transferurilor între actorii publici și privați ([7]), cât și a transferurilor dintre autoritățile publice.

— Între actorii publici și privați:

19. AEPD vede logica aplicabilității unui viitor instrument la transferuri între actorii publici și privați. Dezvoltarea unui astfel de instrument se produce pe fundalul unor solicitări din partea SUA, survenite în ultimii ani, vizând informații provenite de la entități private. AEPD ia notă de faptul că, într-adevăr, actorii privați devin o sursă de informații sistematică în perspectiva aplicării legii, atât la nivelul UE, cât și la nivel internațional ([8]). Cazul Swift a reprezentat un precedent major în care unei companii private i s-a solicitat să transmită date în mod sistematic și masiv autorităților de aplicare a legii dintr-un stat terț ([9]). Colectarea de date din registrele cu numele pasagerilor (PNR) ale companiilor aeriene se încadrează în aceeași logică. În avizul său privind un proiect de decizie-cadru pentru un sistem european al registrelor cu numele pasagerilor (PNR), AEPD a pus deja sub semnul întrebării legitimitatea acestei tendințe ([10]).

20. Există încă două motive suplimentare pentru a manifesta reticență cu privire la includerea transferurilor între actorii publici și privați în domeniul de aplicare al unui viitor instrument.

21. În primul rând, această includere ar putea avea un efect nedorit în interiorul teritoriului Uniunii Europene înseși. AEPD manifestă îngrijorări serioase cu privire la faptul că, în cazul în care datele companiilor private (de tipul instituțiilor financiare) pot fi transferate în principiu către țări terțe, aceasta ar putea provoca o presiune puternică pentru a pune același tip de date în egală măsură la dispoziția autorităților de aplicare a legii, în interiorul UE. Schema PNR este un exemplu de astfel de evoluție nedorită, care a început printr-o colectare masivă a datelor pasagerilor de către SUA, urmând ulterior să fie de asemenea ([11]) transpusă în contextul intern european, fără ca necesitatea și proporționalitatea sistemului să fi fost clar demonstrate.

22. În al doilea rând, în avizul său referitor la propunerea Comisiei privind PNR-UE, AEPD a ridicat, de asemenea, problema cadrului de protecție a datelor (primul sau al treilea pilon) aplicabil condițiilor cooperării între actorii publici și privați: ar trebui ca normele să fie întemeiate

([7]) A se vedea în special capitolul 3 din raport, „Chestiuni nesoluționate care privesc relațiile transatlantice", punctul 1: „Consecvența în cadrul obligațiilor entităților private în timpul transferurilor de date".

([8]) A se vedea cu privire la această chestiune Avizul AEPD din 20 decembrie 2007 referitor la propunerea de decizie-cadru a Consiliului privind utilizarea datelor din registrul cu numele pasagerilor (PNR) în scopul aplicării legii, JO C 110, 1.5.2008, p. 1. „De obicei, a existat o separare clară între activitățile de aplicare a legii și cele ale sectorului privat, prin care activitățile de aplicare a legii sunt executate de autorități special desemnate, în special forțele de poliție, iar actorii privați sunt chemați, în funcție de situație, să comunice date cu caracter personal acestor autorități de aplicare a legii. Există în prezent o tendință de a impune, în mod sistematic, actorilor privați cooperarea în scopul aplicării legii."

([9]) A se vedea Avizul 10/2006 al Grupului de lucru al articolului 29 din 22 noiembrie 2006 privind prelucrarea datelor cu caracter personal de către *Society for Worldwide Interbank Financial Telecommunication* (SWIFT), WP 128.

([10]) Avizul din 20 decembrie 2007, op.cit.

([11]) A se vedea propunerea de decizie-cadru a Consiliului privind utilizarea datelor din registrul cu numele pasagerilor (PNR) în scopul aplicării legii, menționată în nota de subsol 8, astfel cum este discutată în prezent în Consiliu.

pe calitatea operatorului de date (sectorul privat) sau pe scopul urmărit (aplicarea legii)? Linia de demarcare între primul și cel de al treilea pilon este departe de a fi clară în situații în care sunt prevăzute obligații pentru actorii privați cu privire la prelucrarea datelor cu caracter personal în scopul aplicării legii. Este semnificativ în acest context faptul că avocatul general Bot, în avizul său recent privind cazul păstrării datelor ([12]) propune o linie de demarcare pentru aceste situații, adăugând însă următoarele la propunerea sa: „Această linie de demarcare nu este cu siguranță neexpusă criticilor și poate părea artificială în unele privințe." AEPD ia notă, de asemenea, de faptul că hotărârea Curții ([13]) cu privire la PNR nu răspunde în totalitate la întrebarea privitoare la cadrul juridic aplicabil. De exemplu, faptul că anumite activități nu intră sub incidența Directivei 95/46/CE nu înseamnă în mod automat că activitățile respective pot fi reglementate în cadrul celui de al treilea pilon. În consecință, este posibil să persiste o lacună în privința legislației aplicabile, ceea ce generează în orice caz nesiguranță juridică cu privire la garanțiile juridice aflate la dispoziția persoanelor la care se referă datele.

23. În această perspectivă, AEPD subliniază că trebuie să se garanteze faptul că un viitor instrument cu principii generale de protecție a datelor nu poate legitima în sine transferul transatlantic al datelor cu caracter personal între entități publice și private. Acest transfer poate fi inclus doar într-un viitor instrument, cu următoarele condiții:

— viitorul instrument stipulează că transferul este permis doar în cazul în care s-a demonstrat că acesta este absolut necesar într-un anumit scop, care urmează să fie hotărât de la caz la caz;

— transferul în sine este înconjurat de importante măsuri de securitate pentru protecția datelor (precum cele descrise în prezentul aviz).

Mai mult, AEPD ia notă de nesiguranța existentă cu privire la cadrul de protecție a datelor aplicabil și pledează, în orice caz, pentru neincluderea transferului de date cu caracter personal între entități publice și private în stadiul actual al legislației UE.

— Între autoritățile publice:

24. Domeniul de aplicare exact al schimbului de informații este neclar. Ca un prim pas în continuarea activității către un instrument comun, domeniul de aplicare avut în vedere pentru un asemenea instrument ar trebui să fie clarificat. Rămân în special următoarele întrebări:

— În ceea ce privește bazele de date situate în UE, instrumentul ar viza bazele de date centralizate administrate (parțial) de către UE, precum bazele de date ale Europol și Eurojust sau bazele de date descentralizate administrate de către statele membre sau ambele categorii?

— Domeniul de aplicare al instrumentului se extinde la rețelele interconectate, adică garanțiile prevăzute vor acoperi datele care fac obiectul unui schimb între state membre sau agenții, atât în UE, cât și în SUA?

— Instrumentul ar acoperi doar schimbul între bazele de date din domeniul aplicării legii (poliție, justiție, posibil vămi) sau și alte baze de date, cum ar fi cele din domeniul fiscal?

— Instrumentul ar fi pus în legătură și cu bazele de date ale agențiilor de securitate națională sau ar permite accesul acestor agenții la baze de date din domeniul aplicării legii aflate pe teritoriul celeilalte părți contractante (UE pentru SUA și viceversa)?

— Instrumentul ar acoperi transferul de informații de la caz la caz sau va permite accesul permanent la bazele de date existente? Această ultimă ipoteză ar ridica cu siguranță întrebări cu privire la proporționalitate, astfel cum se discută mai jos la capitolul V, punctul 3.

Scopul aplicării legii

25. Definirea scopului unui posibil acord lasă, de asemenea, loc pentru nesiguranță. Scopurile aplicării legii sunt indicate în mod clar în introducere, precum și în primul principiu anexat la raport, urmând să fie analizate mai jos în capitolul IV al prezentului aviz. AEPD ia deja notă de faptul că rezultă din aceste afirmații că schimbul de date s-ar concentra pe chestiuni ce țin de cel de al treilea pilon, dar se poate pune întrebarea dacă aceasta reprezintă doar un prim pas spre un schimb de informații mai amplu. Pare clar faptul că scopurile care țin de „securitatea publică" formulate în raport includ combaterea terorismului, a criminalității organizate și a altor forme de criminalitate. Cu toate acestea, este acesta conceput pentru a permite în egală măsură schimbul de date pentru alte interese publice cum ar fi, eventual, riscurile vizând sănătatea publică?

26. AEPD recomandă restrângerea scopului la prelucrarea de date identificată în mod precis și justificarea alegerilor în materie de politici care duc la o astfel de definire a scopului.

([12]) Avizul avocatului general Bot din 14 octombrie 2008, Irlanda c. Parlamentului European și a Consiliului, (Cauza C-301/06), alineatul 108.

([13]) Hotărârea Curții din 30 mai 2006, Parlamentul European c. Consiliului Uniunii Europene (C-317/04) și Comisia Comunităților Europene (C-318/04, cauzele conexate C-317/04 și C-318/04, Culegere [2006], p. I-4721.

Un spațiu global de securitate transatlantică

27. Scopul general al prezentului raport ar trebui să fie pus în perspectiva spațiului global de securitate transatlantică discutat de așa-numitul „Future Group" ([14]). Raportul acestui grup, emis în iunie 2008, se concentrează într-o anumită măsură pe dimensiunea externă a politicii afacerilor interne. Acesta susține că „până în 2014 Uniunea Europeană ar trebui să se decidă în ceea ce privește obiectivul politic de a realiza, împreună cu Statele Unite, un spațiu de cooperare euro-atlantic în domeniul libertății, securității și justiției." Această cooperare ar depăși securitatea în sesnul strict al termenului și ar include cel puțin subiectele abordate în actualul titlu IV al Tratatului CE precum imigrația, vizele și azilul și cooperarea în materie de drept civil. Trebuie pusă întrebarea în ce măsură un acord privind principii de bază în materie de protecție a datelor, precum cele menționate în raportul GCNÎ, ar putea și ar trebui să reprezinte baza pentru un schimb de informații într-un domeniu atât de extins.

28. În mod normal, până în 2014 structura sub formă de piloni nu va mai exista și va exista un unic temei juridic pentru protecția datelor pe teritoriul Uniunii Europene înseși (în temeiul Tratatului de la Lisabona, articolul 16 din Tratatul privind funcționarea Uniunii Europene). Cu toate acestea, faptul că există armonizare la nivelul UE cu privire la *reglementarea* protecției datelor nu implică faptul că orice acord cu o țară terță ar putea permite *transferul* oricăror date cu caracter personal, indiferent de scop. În funcție de context și de condițiile de prelucrare, garanții adaptate de protecție a datelor ar putea fi necesare pentru domenii specifice precum aplicarea legii. AEPD recomandă luarea în considerare a consecințelor acestor diferite perspective la pregătirea unui viitor acord.

III.2. **Natura acordului**

Cadrul instituțional european

29. Pe termen scurt, în orice caz, este esențială identificarea pilonului în cadrul căruia va fi negociat acordul. Acest lucru este necesar în special datorită cadrului de reglementare internă pentru protecția datelor care va fi afectat de un asemenea acord. Va fi acesta cadrul primului pilon – în principiu Directiva 95/46/CE cu regimul său specific pentru transferul de date către țări terțe – sau va fi cadrul celui de al treilea pilon cu un regim mai puțin strict pentru transferurile către țări terțe? ([15])

30. În timp ce scopurile care țin de aplicarea legii prevalează, după cum s-a menționat deja, raportul GCNÎ menționează totuși colectarea datelor de la actorii privați, iar scopurile pot fi de asemenea interpretate într-un sens larg care ar putea depăși simpla noțiune de securitate, incluzând de exemplu imigrația și chestiunile vizând controlul frontierelor, dar posibil și sănătatea publică. Având în vedere aceste incertitudini, ar fi cu siguranță preferabil să se aștepte armonizarea pilonilor în cadrul legislației UE, astfel cum se prevede în Tratatul de la Lisabona, pentru a se stabili în mod clar temeiul juridic pentru negocieri și rolul precis al instituțiilor europene, în special al Parlamentului European și al Comisiei.

Forța juridică obligatorie a instrumentului

31. Ar trebui să se clarifice dacă concluziile discuțiilor vor duce la un memorandum de înțelegere sau la alt instrument fără forță juridică obligatorie sau dacă acestea vor consta într-un acord internațional cu forță juridică obligatorie.

32. AEPD sprijină preferința pentru un acord cu forță juridică obligatorie menționată în raport. Un acord oficial cu forță juridică obligatorie reprezintă, din punctul de vedere al AEPD, o condiție prealabilă indispensabilă pentru orice transfer de date în afara UE, indiferent de scopul pentru care datele sunt transferate. Niciun transfer de date către o țară terță nu poate avea loc în absența unor condiții adecvate și a a unor măsuri de securitate incluse într-un cadru juridic specific (și cu forță juridică obligatorie). Cu alte cuvinte, un memorandum de înțelegere sau un alt instrument fără forță juridică obligatorie poate fi util pentru a oferi îndrumări cu privire la negocieri în vederea unor acorduri ulterioare cu forță juridică obligatorie, dar nu se poate niciodată substitui nevoii de un acord cu forță juridică obligatorie.

Efect direct

33. Dispozițiile instrumentului ar trebui să prezintă forță juridică obligatorie în egală măsură pentru SUA și UE și statele sale membre.

34. Mai mult, ar trebui să se asigure faptul că persoanele fizice au dreptul de a își exercita drepturile și în special dreptul de a obține accesul la o cale de atac, pe baza principiilor convenite. Conform AEPD, acest rezultat poate fi realizat la modul optim dacă dispozițiile de fond ale instrumentului sunt formulate într-un asemenea mod încât acestea au un efect direct asupra rezidenților din Uniunea Europeană și pot fi invocate în fața unui tribunal. Prin urmare, efectul direct al dispozițiilor acordului internațional, precum și condițiile transpunerii acestuia în legislația europeană internă și în legislația națională în vederea asigurării eficienței măsurilor, trebuie să fie formulate în mod clar în instrument.

Relația cu alte instrumente

35. Măsura în care acordul este autonom sau trebuie să fie completat de la caz la caz de acorduri ulterioare privind schimburi specifice de date este, de asemenea, o chestiune fundamentală. Faptul că un singur acord ar putea acoperi într-un mod adecvat, cu un unic set de standarde,

([14]) Raportul Grupului consultativ informal la nivel înalt privind viitorul politicii europene în domeniul afacerilor interne, „Libertate, securitate, viață privată – Afaceri interne europene într-o lume deschisă", iunie 2008, disponibil la register.consilium.europa.eu

([15]) A se vedea articolele 11 și 13 din Decizia-cadru privind protecția datelor menționată la punctul 7 din prezentul aviz.

multiplele specificități ale prelucrării de date în cadrul celui de al treilea pilon poate fi într-adevăr pus sub semnul întrebării. Există încă și mai multe îndoieli în privința faptului că acesta ar putea *permite*, fără discuții și măsuri de securitate suplimentare, un mecanism generalizat de aprobare a oricărui transfer de date cu caracter personal, indiferent de scopul și de natura datelor respective. În plus, acordurile cu țări terțe nu sunt în mod necesar permanente, deoarece ele pot fi legate de amenințări specifice, pot face obiectul unei revizuiri sau al unor clauze de caducitate. Pe de altă parte, standardele minime comune recunoscute de un instrument cu forță juridică obligatorie ar putea facilita orice discuție ulterioară privind transferul datelor cu caracter personal referitor la o bază de date specifică sau la anumite operațiuni de prelucrare.

36. Prin urmare, AEPD ar privilegia dezvoltarea unui set minim de criterii în materie de protecție a datelor, care ar urma să fie completat de la caz la caz cu dispoziții suplimentare specifice, astfel cum se menționează în raportul GCNÎ, față de alternativa unui acord autonom. Acele dispoziții suplimentare specifice reprezintă o condiție prealabilă pentru a permite transferul de date într-un anumit caz. Aceasta ar încuraja o abordare armonizată în materie de protecție a datelor.

Aplicarea la instrumentele deja existente

37. Ar trebui, de asemenea, examinat modul în care un posibil acord general s-ar combina cu acorduri deja existente încheiate între UE și SUA. Ar trebui notat faptul că aceste acorduri deja existente nu au aceeași forță juridică: demne de menționat în mod special sunt acordul PNR (cel care prezintă cel mai înalt grad de siguranță juridică), acordurile Europol și Eurojust sau schimbul de scrisori SWIFT ([16]). Ar completa un nou cadru general aceste instrumente deja existente sau ar rămâne acestea neatinse, noul cadru aplicându-se doar viitoarelor schimburi de date cu caracter personal? În opinia AEPD, consecvența juridică ar necesita un set armonizat de norme, care să se aplice atât viitoarelor acorduri cu forță juridică obligatorie privind transferurile de date, cât și celor deja existente, precum și să le completeze.

38. Aplicarea acordului general la instrumentele deja existente ar prezenta avantajul de a consolida forța juridică obligatorie a acestora. Acest lucru ar fi extrem de bine-venit în ceea ce privește instrumentele care nu au forță juridică obligatorie, cum ar fi schimbul de scrisori SWIFT, deoarece ar impune cel puțin respectarea unui set de principii generale privind viața privată.

IV. **EVALUARE JURIDICĂ GENERALĂ**

39. Prezentul capitol va examina modul în care trebuie evaluat nivelul de protecție al unui cadru sau instrument specific, incluzând chestiunea criteriilor de referință care trebuie utilizate și cerințele de bază necesare.

([16]) A se vedea nota de subsol nr. 2.

Nivel de protecție adecvat

40. În opinia AEPD, ar trebui să fie clar că unul dintre principalele rezultate ale unui viitor instrument ar fi faptul că transferul de date cu caracter personal către Statele Unite poate avea loc doar în măsura în care autoritățile din Statele Unite garantează un nivel adecvat de protecție (și viceversa).

41. AEPD consideră că doar un test efectiv de evaluare a caracterului adecvat ar asigura garanții suficiente pentru nivelul de protecție a datelor cu caracter personal. AEPD consideră că un acord-cadru general cu un domeniu de aplicare la fel de extins ca cel al raportului GCNÎ ar avea dificultăți în a trece cu succes testul efectiv de evaluare a caracterului adecvat. Caracterul adecvat al acordului general ar putea fi recunoscut doar în cazul în care acesta este combinat cu caracterul adecvat al acordurilor specifice încheiate de la caz la caz.

42. Aprecierea nivelului de protecție furnizat de țări terțe nu reprezintă un exercițiu neobișnuit, în special pentru Comisia Europeană: caracterul adecvat reprezintă în cadrul primului pilon o cerință care trebuie îndeplinită pentru transfer. Acesta a fost măsurat cu multiple ocazii în temeiul articolului 25 din Directiva 95/46/CE pe baza unor criterii specifice, și a fost confirmat de decizii ale Comisiei Europene ([17]). În cadrul celui de al treilea pilon, un asemenea sistem nu este prevăzut în mod explicit: măsurarea caracterului adecvat al protecției este prescrisă doar în situația specifică a articolelor 11 și 13 din Decizia-cadru privind protecția datelor ([18]) (neadoptată încă) și este lăsată la latitudinea statelor membre.

43. În cazul de față, domeniul de aplicare al exercițiului are incidență asupra scopurilor ce vizează aplicarea legii, iar discuțiile sunt conduse de către Comisie sub supravegherea Consiliului. Contextul este diferit de evaluarea principiilor „Safe Harbour" sau de caracterul adecvat al legislației canadiene, și prezintă mai multe conexiuni cu negocierile recente privind PNR cu SUA și Australia, desfășurate în cadrul juridic al celui de al treilea pilon. Cu toate acestea, principiile GCNÎ au fost de asemenea menționate în contextul Programului de scutire de vize („Visa Waiver Programme"), care vizează frontierele și imigrația și, prin urmare, chestiuni ce țin de primul pilon.

44. AEPD recomandă ca orice examinare a caracterului adecvat realizată în cadrul unui viitor instrument să se întemeieze pe experiențele înregistrate în aceste domenii diverse. AEPD

([17]) Decizii ale Comisiei privind caracterul adecvat al protecției datelor cu caracter personal în țări terțe, incluzând Argentina, Canada, Elveția, Statele Unite, Guernsey, Insula Man și Jersey, sunt disponibile la http://ec.europa.eu/justice_home/fsj/privacy/thridcountries/index_en.htm

([18]) Limitată la transferul către o țară terță sau un organism internațional din partea unui stat membru a unor date primite din partea unei autorități competente din alt stat membru.

recomandă, de asemenea, dezvoltarea în continuare a noțiunii de „caracter adecvat" în contextul unui viitor instrument, pe baza unor criterii similare, astfel cum au fost utilizate în determinările anterioare ale caracterului adecvat.

Recunoaștere reciprocă – reciprocitate

45. Cel de al doilea element al nivelului de protecție vizează recunoașterea reciprocă a sistemelor UE și SUA. Raportul GCNÎ menționează în această privință că obiectivul ar fi de a „obține recunoașterea eficienței sistemelor de protecție a vieții private și a datelor ale celeilalte părți pentru domeniile acoperite de principiile respective" ([19]), și de a obține o „aplicare echivalentă și reciprocă a legislației în materie de protecție a vieții private și a datelor cu caracter personal".

46. Este evident pentru AEPD că recunoașterea reciprocă (sau reciprocitatea) poate fi posibilă doar în cazul în care este garantat un nivel adecvat de protecție. Cu alte cuvinte, viitorul instrument ar trebui să armonizeze un nivel minim de protecție (prin intermediul examinării caracterului adecvat, luând în considerare nevoia de acorduri specifice de la caz la caz). Reciprocitatea ar putea fi recunoscută doar cu îndeplinirea acestei condiții prealabile.

47. Primul element care trebuie luat în considerare este reciprocitatea dispozițiilor de fond în materie de protecție a datelor. În opinia AEPD, un acord ar trebui să abordeze noțiunea reciprocității dispozițiilor de fond în materie de protecție a datelor într-un mod care să garanteze, pe de o parte, faptul că prelucrarea datelor în cadrul teritoriului UE (și al SUA) respectă pe deplin legislațiile naționale în materie de protecție a datelor, și pe de altă parte faptul că prelucrarea în afara țării de origine a datelor care intră sub incidența acordului respectă principiile de protecție a datelor prevăzute în acord.

48. Cel de al doilea element este reciprocitatea mecanismelor privind căile de atac. Ar trebui să se asigure faptul că cetățenii europeni dispun de o cale de atac adecvată atunci când datele care îi vizează sunt prelucrate în Statele Unite (indiferent de legislația care se aplică respectivei prelucrări), dar, în egală măsură, și faptul că Uniunea Europeană și statele sale membre conferă drepturi echivalente cetățenilor SUA.

49. Cel de al treilea element este reciprocitatea accesului la datele cu caracter personal pentru autoritățile de aplicare a legii. În cazul în care un instrument le permite autorităților Statelor Unite accesul la date originare din Uniunea Europeană, reciprocitatea ar implica că același acces ar trebui să le fie acordat autorităților UE, cu privire la datele originare din SUA. Reciprocitatea nu trebuie să aducă atingere eficienței protecției persoanei la care se referă datele. Aceasta este o condiție prealabilă pentru a le permite accesul „transatlantic" autorităților de aplicare a legii. În termeni concreți, aceasta înseamnă că:

— Accesul direct al autorităților Statelor Unite la date de pe teritoriul UE (și viceversa) nu ar trebui să fie permis. Accesul ar trebui să fie acordat doar într-o manieră indirectă, în cadrul unui sistem de tip „push";

— Accesul ar trebui să aibă loc doar sub controlul autorităților de protecție a datelor și al autorităților judiciare din țara unde are loc prelucrarea datelor;

— Accesul autorităților Statelor Unite la baze de date de pe teritoriul UE ar trebui să respecte dispozițiile de fond privind protecția datelor (a se vedea mai sus) și să garanteze căi de atac depline pentru persoana la care se referă datele.

Precizia instrumentului

50. Specificarea condițiilor evaluării (caracterul adecvat, echivalența, recunoașterea reciprocă) este esențială, deoarece aceasta determină conținutul, în termeni de precizie, siguranță juridică și eficiență a protecției. Conținutul unui viitor instrument trebuie să fie precis și exact.

51. Pe lângă aceasta, ar trebui să fie clar faptul că orice acord specific încheiat într-o etapă ulterioară va trebui în continuare să includă măsuri de securitate detaliate și complete în materie de protecție a datelor cu privire la subiectul schimbului de date preconizat. Doar un asemenea nivel dublu de principii concrete în materie de protecție a datelor ar garanta „apropierea" necesară între acordul general și acordurile specifice, după cum s-a menționat deja la punctul 35, respectiv punctul 36 al prezentului aviz.

Elaborarea unui model pentru alte țări terțe

52. Măsura în care un acord cu Statele Unite ar putea reprezenta un model pentru alte țări terțe merită o atenție deosebită. AEPD ia notă de faptul că, pe lângă SUA, raportul anterior menționat al Grupului consultativ informal la nivel înalt privind viitorul politicii europene în domeniul afacerilor interne („Grupul Future") menționează de asemenea Rusia ca partener strategic al UE. În măsura în care principiile sunt neutre și respectă măsurile de securitate fundamentale ale UE, acestea ar putea constitui un precedent util. Cu toate acestea, specificitățile legate de exemplu de cadrul legal al țării de destinație sau de scopul transferului ar împiedica simpla transpunere a acordului. La fel de decisivă va fi și situația democratică a țărilor terțe: ar trebui să se asigure garantarea și punerea în aplicare efectivă a principiilor convenite în țara de destinație.

Ce criterii de referință trebuie utilizate pentru evaluarea nivelului de protecție?

53. Un caracter adecvat implicit sau explicit ar trebui în orice caz să respecte cadrul juridic internațional și european și

([19]) Capitolul A. Acord internațional cu forță juridică obligatorie, p. 8.

în special măsurile de securitate pentru protecția datelor convenite de comun acord. Acestea sunt consacrate în liniile directoare ale Organizației Națiunilor Unite, Convenția 108 a Consiliului Europei și protocolul adițional la aceasta, liniile directoare ale OCDE și proiectul de decizie-cadru privind protecția datelor, precum și, pentru chestiuni ce țin de primul pilon, în Directiva 95/46/CE ([20]). Toate aceste instrumente conțin principii similare care sunt recunoscute pe plan mai larg ca fiind nucleul de bază al protecției datelor cu caracter personal.

54. Este cu atât mai important ca principiile sus-menționate să fie luate în considerare în mod corespunzător, având în vedere impactul unui eventual acord precum cel prevăzut de raportul GCNÎ. Un instrument care abordează întregul sector de *aplicare a legii* dintr-o țară terță ar reprezenta, într-adevăr, o situație fără precedent. Deciziile privind caracterul adecvat existente în cadrul primului pilon și acordurile încheiate cu țări terțe în cadrul celui de al treilea pilon al UE (Europol, Eurojust) au fost întotdeauna conectate cu un transfer specific de date, în timp ce în cazul de față ar putea deveni posibile transferuri cu un domeniu de aplicare mult mai larg, având în vedere obiectivul extins urmărit (combaterea infracțiunilor penale, securitatea națională și publică, aplicarea legii la frontiere) și numărul necunoscut de baze de date implicate.

Cerințe de bază

55. Condițiile care trebuie îndeplinite în contextul transferului de date cu caracter personal către țările terțe au fost dezvoltate într-un document de lucru al Grupului de lucru al articolului 29 ([21]). Orice acord privind principiile minime referitoare la viața privată ar trebui să treacă un test de respectare a cerințelor care să asigure eficacitatea măsurilor de securitate pentru protecția datelor.

— La nivel material: principiile privind protecția datelor ar trebui să furnizeze un nivel ridicat de protecție și să respecte standardele în conformitate cu principiile UE. Cele 12 principii incluse în raportul GCNÎ vor fi analizate în mod mai detaliat din această perspectivă în capitolul V din prezentul aviz.

— La nivelul specificității: în funcție de natura acordului și în special dacă este vorba despre un acord internațional oficial, normele și procedurile ar trebui să fie suficient de detaliate, pentru a permite o punere în aplicare eficace.

— La nivel de supraveghere: pentru a se garanta respectarea normelor convenite, ar trebui instituite mecanisme de control specifice, atât la nivel intern (audit), cât și extern (revizuiri). Respectivele mecanisme ar trebui să fie disponibile pentru ambele părți la acord. Supravegherea include mecanisme de garantare a respectării cerințelor la nivel macro precum mecanismele comune de revizuire, precum și de garantare a respectării cerințelor la nivel micro, de tipul căilor de atac individuale.

56. În afară de aceste trei cerințe de bază, o atenție deosebită ar trebui acordată specificităților legate de prelucrarea datelor cu caracter personal în contextul aplicării legii. Într-adevăr, acesta reprezintă un domeniu în care drepturile fundamentale pot suferi o serie de restricții. Așadar ar trebui adoptate măsuri de securitate care să compenseze restricționarea drepturilor individuale, în special în privința următoarelor aspecte, avându-se în vedere impactul asupra persoanei:

— Transparența: informația și accesul la datele cu caracter personal în contextul aplicării legii ar putea fi limitate, datorită, de exemplu, necesității unor anchete discrete. În timp ce în cadrul UE, în mod tradițional, mecanisme suplimentare sunt instituite pentru a compensa respectiva limitare a drepturilor fundamentale (care implică adesea autorități independente de protecție a datelor), trebuie să se garanteze faptul că mecanisme similare de compensare vor fi disponibile în momentul în care informația este transferată spre o țară terță.

— Căi de atac: pentru motivele sus-menționate, persoanele fizice ar trebui să beneficieze de posibilități alternative de a-și apăra drepturile, în special prin intermediul unei autorități independente de supraveghere și în fața unui tribunal.

— Păstrarea datelor: este posibil ca justificarea pentru perioada de păstrare să nu fie transparentă. Trebuie adoptate măsuri astfel încât acest lucru să nu împiedice exercitarea eficace a drepturilor de către persoanele la care se referă datele sau de către autoritățile de supraveghere.

([20]) — Liniile directoare ale Organizației Națiunilor Unite privind prelucrarea informatizată a datelor cu caracter personal, adoptate de Adunarea Generală din 14 decembrie 1990, disponibile la www.unhchr.ch/html/menu3/b/71.htm
— Convenția Consiliului Europei pentru protecția persoanelor cu privire la prelucrarea automată a datelor cu caracter personal din 28 ianuarie 1981, disponibilă la www.conventions.coe.int/treaty/en/Treaties/html/108.htm
— Liniile directoare ale OCDE privind protecția vieții private și fluxul transfrontalier de date cu caracter personal, adoptate la 23 septembrie 1980, disponibile la www.oecd.org/document/20/0,3343,en_2649_34255_15589524_1_1_1_1,00.html
— Proiectul de decizie-cadru a Consiliului privind protecția datelor cu caracter personal prelucrate în cadrul cooperării polițienești și judiciare în materie penală, disponibil la http://ec.europa.eu/prelex/detail_dossier_real.cfm?CL=en&DosId=193371
— 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, JO L 281, 23.11.1995, p. 31.

([21]) Documentul de lucru din 24 iulie 1998 privind Transferurile de date cu caracter personal către țările terțe: aplicarea articolelor 25 și 26 din directiva UE privind protecția datelor; WP12.

— Răspunderea autorităților de aplicare a legii: în absența unei transparențe eficace, mecanismele de control aflate la dispoziția fie a persoanelor fizice, fie a actorilor instituționali, nu pot în niciun caz să se aplice în mod exhaustiv. Ar fi de asemenea de importanță crucială ca astfel de controale să fie instituite în mod ferm, avându-se în vedere caracterul sensibil al datelor și măsurile coercitive care pot fi luate împotriva persoanelor fizice pe baza prelucrării datelor. Răspunderea reprezintă un aspect decisiv în privința mecanismelor naționale de control ale țării de destinație, dar și în privința posibilităților de revizuire de care dispune țara sau regiunea de origine a datelor. Astfel de mecanisme de revizuire sunt prevăzute în acorduri specifice precum acordul PNR, iar AEPD recomandă de asemenea în mod ferm includerea acestora în instrumentul general.

V. **ANALIZA PRINCIPIILOR**

Introducere

57. Prezentul capitol analizează cele 12 principii incluse în documentul GCNÎ din următoarea perspectivă:

— Aceste principii demonstrează faptul că SUA și UE au o serie de opinii comune referitoare la nivelul principiilor, întrucât pot fi constatate similarități cu principiile Convenției 108.

— Cu toate acestea, un acord la nivel de principiu nu este suficient. Un instrument juridic ar trebui să fie suficient de puternic pentru a asigura respectarea sa.

— AEPD regretă faptul că principiile nu sunt însoțite de un memorandum explicativ.

— Înainte de a începe descrierea principiilor, ar trebui să fie clar faptul că ambele părți înțeleg în același fel formulările utilizate, de exemplu în privința noțiunii de informații cu caracter personal sau de persoane fizice protejate. Ar fi bine-venite definiții în acest sens.

1. Specificarea scopului

58. Primul principiu menționat în anexa la raportul GCNÎ arată faptul că informațiile cu caracter personal sunt prelucrate pentru scopuri legitime de aplicare a legii. Așa cum se menționează anterior, în cazul Uniunii Europene, acest lucru se referă la prevenirea, depistarea, cercetarea sau urmărirea infracțiunilor penale. Cu toate acestea, pentru SUA, interpretarea aplicării legii depășește infracțiunile penale și include „scopuri vizând aplicarea legii la frontiere, securitatea publică și națională”. Consecințele unor astfel de discrepanțe între scopurile declarate ale UE și cele ale SUA nu sunt clare. Întrucât raportul menționează faptul că în practică scopurile pot coincide în mare măsură, este de o importanță decisivă să se știe precis în ce măsură acestea *nu* coincid. În domeniul aplicării legii, având în vedere impactul măsurilor adoptate asupra persoanelor fizice, principiul limitării scopurilor trebuie respectat cu strictețe, iar scopurile declarate trebuie să fie clare și circumscrise. Luând în considerare reciprocitatea avută în vedere în raport, aproximarea respectivelor scopuri pare de asemenea esențială. Pe scurt, este nevoie de o clarificare modului în care este înțeles acest principiu.

2. Integritatea/calitatea datelor

59. AEPD salută dispoziția care solicită informații cu caracter personal exacte, relevante, oportune și complete, după cum este necesar pentru prelucrarea conform legii. Un astfel de principiu reprezintă o condiție de bază pentru o prelucrare eficientă a datelor.

3. Necesitate/proporționalitate

60. Principiul arată o legătură clară între informațiile colectate și necesitatea ca respectivele informații servească unui scop referitor la aplicarea legii, prevăzut de un act legislativ. Cerința unui temei juridic reprezintă un element pozitiv care asigură legitimitatea prelucrării. Cu toate acestea, AEPD ia act de faptul că, deși acest lucru consolidează siguranța juridică a prelucrării, temeiul juridic al unei astfel de procesări îl reprezintă un act legislativ al unei țări terțe. Un act legislativ al unei țări terțe nu poate reprezenta în sine un temei legitim pentru transferul datelor cu caracter personal ([22]). În contextul raportului GCNÎ, pare să se prezume faptul că legitimitatea actului legislativ al unei țări terțe, de exemplu Statele Unite, este recunoscută în principiu. Ar trebui să se aibă în vedere faptul că, dacă un asemenea raționament își poate găsi justificarea în acest caz, considerând ca Statele Unite sunt un stat democratic, respectiva schemă nu poate fi valabilă și nu ar putea fi transpusă în relațiile cu orice alte țări terțe.

61. Orice transfer de date cu caracter personal trebuie să fie relevant, necesar și adecvat în conformitate cu anexa la raportul GCNÎ. AEPD subliniază faptul că, pentru a fi proporțională, prelucrarea nu trebuie să fie inutil de intruzivă, iar modalitățile acesteia trebuie să fie echilibrate, luând în considerare drepturile și interesele persoanelor la care se referă datele.

62. Din acest motiv, accesul la informații ar trebui să aibă loc numai după o apreciere de la caz la caz, în funcție de necesitățile practice din contextul unei cercetări specifice. Accesul permanent al autorităților de aplicare a legii din țările terțe la bazele de date situate în UE ar fi considerat

([22]) A se vedea în special articolul 7 literele (c) și (e) din Directiva 95/46/CE. În avizul său 6/2002 din 24 octombrie 2002 privind transmiterea informațiilor din listele de pasageri și a altor date de către liniile aeriene Statelor Unite ale Americii, Grupul de lucru al articolului 29 a arătat că „nu pare acceptabil ca o decizie unilaterală adoptată de o țară terță pentru motive care țin de propriul său interes public să conducă la transferul de rutină al tuturor datelor care intră sub incidența protecției oferite de directivă”.

disproporționat și insuficient justificat. AEPD reamintește că, chiar în contextul acordurilor existente referitoare la schimbul de date, de exemplu în cazul acordului PNR, schimbul de date se bazează pe circumstanțe specifice și se desfășoară pe o perioadă limitată de timp ([23]).

63. Urmând aceeași logică, perioada de păstrare a datelor ar trebui să fie relglementată: datele ar trebui păstrate numai atât timp cât acest lucru este necesar, avându-se în vedere scopul specific urmărit. În cazul în care datele nu mai sunt relevante cu privire la scopul identificat, acestea ar trebui eliminate. AEPD se opune în mod ferm constituirii unor depozite de date în care informații privind persoane fizice nesuspectate să poată fi stocate în vederea unei eventuale necesități viitoare.

4. Securitatea informațiilor

64. În cadrul principiilor se dezvoltă de asemenea măsuri și proceduri care să protejeze datele împotriva utilizării incorecte, a modificării sau a altor riscuri, precum și o dispoziție care limitează accesul la persoanele autorizate. AEPD consideră acest lucru satisfăcător.

65. În plus, principiul ar putea fi completat printr-o dispoziție care să menționeze că ar trebui păstrate registre cu persoanele care accesează datele. Aceasta ar consolida eficacitatea măsurilor de securitate privind limitarea accesului și prevenirea utilizării incorecte a datelor.

66. În plus, ar trebui prevăzută informarea reciprocă în caz de încălcare a securității: destinatarii din SUA, precum și cei din UE, ar fi responsabili de informarea omologilor lor în cazul în care datele primite au făcut obiectul unei divulgări ilegale. Acest lucru va contribui la o responsabilitate consolidată către o prelucrare sigură a datelor.

5. Categorii speciale de informații cu caracter personal

67. Principiul interzicerii prelucrării datelor sensibile este, în opinia AEPD, diminuat în mod considerabil de excepția care permite orice prelucrare a datelor sensibile pentru care legislația națională prevede „măsuri de securitate corespunzătoare". Tocmai din cauza caracterului sensibil al datelor, orice derogare de la principiul interzicerii trebuie să fie justificată în mod adecvat și precis, cu o listă de scopuri și circumstanțe în care un tip identificat de date sensibile poate fi prelucrat, precum și cu o indicare a calității operatorilor care au dreptul de a prelucra astfel de date. Printre măsurile de securitate care urmează să fie adoptate, AEPD consideră că datele sensibile nu ar trebui considerate un element care ar putea declanșa o cercetare. Acestea ar putea fi disponibile în anumite circumstanțe, dar numai în calitate de informații suplimentare cu privire la o persoană la care se referă datele aflată deja în cercetare. Aceste măsuri de securitate și condiții trebuie enumerate în mod limitativ în textul principiului.

6. Răspundere

68. Astfel cum a fost dezvoltat la punctele 55-56 ale prezentului aviz, trebuie asigurată răspunderea entităților publice care prelucrează datele cu caracter personal într-un mod eficace, și trebuie prevăzute asigurări în cadrul acordului referitoare la modalitatea în care va fi asigurată respectiva răspundere. Acest lucru este cu atât mai important cu cât se are în vedere lipsa transparenței asociată în mod tradițional cu prelucrarea datelor cu caracter personal în contextul aplicării legii. În acest sens, menționarea – astfel cum este cazul în prezent în anexă – a faptului că entitățile publice sunt ținute responsabile fără a alte explicații suplimentare privind modalitățile și consecințele unei astfel de răspunderi, nu reprezintă o garanție satisfăcătoare. AEPD recomandă menționarea unei astfel de explicații în textul instrumentului.

7. Supraveghere independentă și eficace

69. AEPD sprijină pe deplin includerea unei dispoziții care să prevadă o supraveghere independentă și eficace, de către una sau mai multe autorități publice de supraveghere. AEPD consideră că ar trebui fie arătat în mod clar cum se interpretează independența, în special față de cine respectivele autorități sunt independente și către cine prezintă rapoarte. În acest sens sunt necesare criterii, care să ia în considerare independența instituțională și funcțională, în relația cu organismele executive și legislative. AEPD reamintește faptul că acesta reprezintă un element esențial pentru a asigura respectarea eficace a principiilor convenite. Competențele de intervenție și de asigurare a aplicării legii ale acestor autorități sunt de asemenea cruciale în raport cu problema răspunderii entităților publice de prelucrare a datelor cu caracter personal, după cum se arată mai sus. Existența și competențelor lor ar trebui să fie vizibile în mod clar pentru persoanele la care se referă datele, pentru a le permite acestora să își exercite drepturile, în special dacă o serie de autorități sunt competente în funcție de contextul prelucrării.

70. Mai mult, AEPD recomandă ca un viitor acord să prevadă de asemenea mecanisme de cooperare între autoritățile de supraveghere.

8. Accesul individual și rectificarea

71. Sunt necesare garanții specifice atunci când este vorba de acces și rectificare în contextul aplicării legii. În acest sens, AEPD salută principiul care afirmă că persoanelor fizice li se furnizează/ar trebui să li se furnizeze accesul la informațiile cu caracter personal care îi vizează și mijloacele de a obține „rectificarea și/sau eliminarea informațiilor cu caracter personal care îi vizează". Cu toate acestea, rămân

([23]) Acordul expiră și încetează să producă efecte la șapte ani de la data semnării, cu excepția cazului în care părțile decid de comun acord să îl înlocuiască.

o serie de incertitudini în privința definiției persoanelor fizice (toate persoanele la care se referă datele ar trebui să fie protejate și nu numai cetățenii țării în cauză) și a condițiilor în care persoanele fizice ar putea să obiecteze cu privire la prelucrarea informațiilor care îi vizează. Sunt necesare precizări cu privire la „cazurile adecvate" în care ar putea sau nu să fie formulată o obiecție. Pentru persoanele la care se referă datele ar trebui fie clar în ce împrejurări – de exemplu, în funcție de tipul autorității, de tipul cercetării sau de alte criterii – își vor putea exercita aceste drepturi.

72. În plus, dacă nu există nicio posibilitate directă de a obiecta față de o prelucrare pentru motive întemeiate, ar trebui să fie posibilă o verificare indirectă, prin intermediul autorității independente care răspunde de supravegherea prelucrării.

9. Transparența și notificarea

73. AEPD evidențiază încă o dată importanța transparenței eficace, pentru a permite persoanelor fizice să își exercite drepturile și să contribuie la răspunderea generală a autorităților publice care prelucrează datele. AEPD sprijină principiile astfel cum au fost redactate și insistă în special asupra necesității unei notificări generale *și* individuale a persoanei fizice în cauză. Acest lucru se reflectă în principiul formulat la punctul 9 al anexei.

74. Cu toate acestea, raportul, la capitolul 2, A. B („Principii convenite") menționează că în SUA transparența poate include „în mod individual sau împreună, publicarea în registrul federal, notificarea individuală și divulgarea în cadrul procedurilor din instanță". Trebuie să fie clar faptul că o publicare într-un monitor oficial nu este suficientă în sine pentru a garanta informarea corespunzătoare a persoanei la care se referă datele. În plus față de notificarea individuală, AEPD reamintește că informațiile trebuie furnizate într-o formă și în termeni care să poată fi înțelese cu ușurință de către persoana la care se referă datele.

10. Căi de atac

75. Pentru a garanta exercitarea eficace a drepturilor lor, persoanele fizice trebuie să poată să înainteze o plângere unei autorități independente de protecție a datelor, precum și să dispună de o cale de atac în fața unei instanțe imparțiale și independente. Ambele posibilități de atac ar trebui să fie disponibile în egală măsură.

76. Accesul la o autoritate independentă de protecție a datelor este necesar întrucât furnizează o asistență flexibilă și mai puțin costisitoare, într-un context – aplicarea legii – care poate fi mai degrabă opac pentru persoanele fizice. Autoritățile de protecție a datelor pot furniza, de asemenea, asistență prin exercitarea drepturilor de acces în numele persoanelor la care se referă datele, în situația în care excepțiile le împiedică pe acestea din urmă să aibă acces direct la datelor cu caracter personal care îi vizează.

77. Accesul la sistemul judiciar reprezintă o garanție suplimentară și indispensabilă a faptului că persoanele la care se referă datele pot apela la o cale de atac în fața unei autorități care aparține unei ramuri a sistemului democratic distinctă față de instituțiile publice care prelucrează de fapt datele care îi vizează. O astfel de cale de atac eficace în fața unei instanțe a fost considerată de Curtea Europeană de Justiție ([24]) ca fiind „esențială pentru a asigura persoanei fizice protecția eficace a dreptului său. (…) [Aceasta] reflectă un principiu general al dreptului comunitar care stă la baza tradițiilor constituționale comune ale statelor membre și a fost consacrat în articolele 6 și 13 din Convenția europeană pentru protecția drepturilor omului și a libertăților fundamentale." Existența unei căi de atac judiciare este de asemenea prevăzută în mod explicit în articolul 47 din Carta Drepturilor Fundamentale a Uniunii Europene și în articolul 22 din Directiva 95/46/CE, fără a aduce atingere oricărei căi de atac administrative.

11. Deciziile individuale automatizate

78. AEPD salută dispoziția care prevede măsuri de securitate adecvate în cazul prelucrării automatizate a informațiilor cu caracter personal. AEPD remarcă că o modalitate comună de înțelegere a ceea ce se consideră a fi „o acțiune care prejudiciază în mod semnificativ interesele relevante ale persoanei" ar clarifica condițiile de aplicare a prezentului principiu.

12. Transferurile ulterioare

79. Condițiile fixate pentru transferurile ulterioare sunt neclare pentru o parte dintre acestea. În special, în cazul în care un transfer ulterior trebuie să respecte acorduri internaționale și acorduri între țările de origine și de destinație, ar trebui să se specifice dacă aceasta se referă la acorduri între cele două țări care au inițiat primul transfer sau la cele două țări implicate în transferul ulterior. În conformitate cu AEPD, acordurile între două țări care au inițiat primul transfer sunt în orice caz necesare.

80. AEPD ia act de asemenea de o definiție foarte largă a „intereselor publice legitime" care permit un transfer ulterior. Domeniul de aplicare al securității publice rămâne neclar, iar extinderea transferurilor în cazul nerespectării eticii sau al profesiilor reglementate pare să fie nejustificată și excesivă în contextul aplicării legii.

VI. **CONCLUZIE**

81. AEPD salută activitatea comună a autorităților UE și SUA în domeniul aplicării legii în cadrul căruia protecția datelor este crucială. Cu toate acestea, AEPD dorește să insiste asupra faptului că această chestiune este complexă, în privința domeniului de aplicare precis și a naturii precise a acesteia, și că prin urmare acesta necesită o analiză atentă

([24]) Cauza 222/84 *Johnston* [1986] Culegere 1651; Cauza 222/86 *Heylens* [1987] Culegere 4097; Cauza C-97/91 *Borelli* [1992] Culegere I-6313).

și aprofundată. Impactul unui instrument transatlantic privind protecția datelor ar trebui examinat cu atenție în legătură cu cadrul juridic existent și cu consecințele asupra cetățenilor.

82. AEPD solicită o mai mare claritate și dispoziții concrete în special cu privire la următoarele aspecte:

— clarificarea naturii instrumentului, care ar trebui să aibă forță juridică obligatorie pentru a oferi o siguranță juridică suficientă;

— o examinare aprofundată a caracterului adecvat, bazată pe cerințe esențiale care să abordeze aspecte ale schemei privind caracterul material, specificitatea și supravegherea. AEPD consideră că caracterul adecvat al instrumentului general ar putea fi recunoscut doar în cazul în care acesta este combinat cu acorduri specifice adecvate, de la caz la caz;

— un domeniu de aplicare circumscris, cu o definire clară și comună a scopurilor vizând aplicarea legii aflate în joc;

— precizări privind modalitățile în conformitate cu care entitățile private ar putea fi implicate în schemele de transfer de date;

— respectarea principiului proporționalității, ceea ce implică schimbul de date în funcție de o apreciere de la caz la caz, în situația în care există o necesitate concretă;

— mecanisme solide de supraveghere și mecanisme de atac aflate la dispoziția persoanelor la care se referă datele, incluzând căi de atac administrative și judiciare;

— măsuri eficace care să garanteze tuturor persoanelor la care se referă datele, indiferent de naționalitatea lor, posibilitatea de a își exercita drepturile;

— implicarea autorităților independente de protecție a datelor, în special în legătură cu supravegherea și asistența acordată persoanelor la care se referă datele.

83. AEPD insistă asupra faptului că ar trebui evitată orice grabă în elaborarea principiilor, întrucât ar duce numai la soluții nesatisfăcătoare, cu efecte opuse celor avute în vedere în termeni de protecție a datelor. În stadiul actual, calea optimă de urmat ar consta așadar în elaborarea unei foi de parcurs către un posibil acord la o etapă ulterioară.

84. AEPD solicită, de asemenea, o mai mare transparență în privința procesului de elaborare a principiilor privind protecția datelor. Instrumentul ar putea beneficia de o dezbatere democratică și ar putea câștiga susținerea și recunoașterea necesare numai cu implicarea tuturor actorilor interesați, incluzând Parlamentul European.

Adoptat la Bruxelles, 11 noiembrie 2008.

Peter HUSTINX

Autoritatea Europeană pentru Protecția Datelor