

Avizul Autorității Europene pentru Protecția Datelor privind propunerea de decizie a Consiliului privind încheierea Acordului dintre Uniunea Europeană și Statele Unite ale Americii privind prelucrarea și transferul datelor de mesagerie financiară din Uniunea Europeană către Statele Unite ale Americii în cadrul Programului de urmărire a finanțării în scopuri teroriste (TFTP II)

(2010/C 355/02)

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 articolul 8,

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

având în vedere solicitarea unui aviz formulată în conformitate cu articolul 28 alineatul (2) din Regulamentul (CE) nr. 45/2001 privind protecția persoanelor fizice cu privire la prelucrarea datelor cu caracter personal de către instituțiile și organele comunitare și privind libera circulație a acestor date ⁽²⁾,

ADOPTĂ PREZENTUL AVIZ:

I. INTRODUCERE

1. La 15 iunie 2010, Comisia a adoptat o propunere de decizie a Consiliului privind încheierea Acordului dintre Uniunea Europeană și Statele Unite ale Americii privind prelucrarea și transferul datelor de mesagerie financiară din Uniunea Europeană către Statele Unite ale Americii în cadrul Programului de urmărire a finanțării în scopuri teroriste (TFTP) (denumită în continuare „propunerea”). Propunerea (inclusiv textul unui proiect de acord cu Statele Unite) a fost transmisă către AEPD în vederea consultării. AEPD salută această consultare și recomandă includerea în preambulul propunerii a unei trimiteri la prezentul aviz.
2. Propunerea Comisiei este determinată de schimbările din cadrul arhitecturii SWIFT ⁽³⁾ care, începând cu 1 ianuarie 2010, asigură că mesajele SWIFT privind tranzacțiile financiare din interiorul Spațiului Economic European și Elveția vor rămâne în zona europeană – spre deosebire de zona transatlantică – și nu vor mai fi transpuse în centrul operațional din SUA.
3. Prin propunerea actuală, Comisia are în vedere încheierea unui acord internațional între UE și SUA, care, în baza articolelor 216 (acorduri internaționale), 82 (cooperare judiciară) și 87 (cooperare polițienească) din Tratatul privind funcționarea Uniunii Europene, ar impune

⁽¹⁾ JO L 281, 23.11.1995, p. 31.

⁽²⁾ JO L 8, 12.1.2001, p. 1.

⁽³⁾ SWIFT este o societate cu sediul în Belgia care furnizează servicii de mesagerie pentru instituțiile financiare la nivel global. Din anul 2001, Departamentul de Trezorerie al SUA a adresat citații administrative către SWIFT pentru a accesa unele dintre datele cu caracter personal privind tranzacțiile financiare, transpuse pe un server situat pe teritoriul SUA.

transferul către Departamentul de Trezorerie al Statelor Unite ale Americii al datelor relevante de mesagerie financiară necesare pentru Programul de urmărire a finanțării în scopuri teroriste al acestui departament.

4. În special, în urma deciziei Parlamentului European din 11 februarie 2010 de a refuza să își dea aprobarea în legătură cu acordul interimar semnat la 30 noiembrie 2009, noul proiect își propune să abordeze în special preocupările legate de protecția datelor cu caracter personal, un drept fundamental care, după intrarea în vigoare a Tratatului de la Lisabona, a dobândit și mai multă relevanță în cadrul juridic al Uniunii Europene.

5. Propunerea evidențiază importanța protecției datelor, făcând în mod explicit trimitere la articolele relevante din tratate și alte instrumente internaționale și recunoscând natura sa de drept fundamental. Cu toate acestea, nu se are în vedere utilizarea articolului 16 din Tratatul privind funcționarea Uniunii Europene ca temei juridic, în ciuda faptului că articolul 1.1 din acordul propus subliniază faptul că unul dintre principalele sale scopuri îl reprezintă asigurarea unui nivel ridicat de protecție a datelor. În această privință, AEPD reiterează faptul că acest acord nu se referă doar la schimbul de date cu caracter personal, ci și la protecția acestor date. Prin urmare, articolul 16 din Tratatul privind funcționarea Uniunii Europene nu este mai puțin relevant ca temei juridic decât articolele 82 și 87 din Tratatul privind funcționarea Uniunii Europene referitoare la cooperarea în domeniul aplicării legii, care au fost alese ca temeiuri juridice.

6. Propunerea este supusă procedurii prevăzute la articolul 218 alineatul (6) din Tratatul privind funcționarea Uniunii Europene. Conform acestei proceduri, Consiliul poate adopta doar o decizie prin care să autorizeze încheierea acordului, după obținerea aprobării Parlamentului European. Astfel, această propunere reprezintă un precedent esențial în cadrul aplicării noilor proceduri de la Lisabona în cazul unui acord internațional privind protecția datelor cu caracter personal. Faptul că în acest acord sunt prevăzute în mod satisfăcător principiile și garanțiile privind protecția datelor cu caracter personal va pregăti terenul necesar pentru aplicarea cu succes a acestora în cadrul altor negocieri.

7. În acest context, AEPD subliniază importanța negocierilor în scopul încheierii unui acord între Uniunea Europeană și Statele Unite ale Americii privind protecția datelor cu caracter personal, atunci când sunt transferate și prelucrate în scopul prevenirii, investigării, detectării sau urmăririi penale a infracțiunilor, inclusiv a actelor de terorism, în cadrul cooperării polițienești sau cooperării judiciare în materie penală. Proiectul de mandat pentru demararea acestor negocieri a fost adoptat de către Comisie la 26 mai 2010. În cadrul prezentării acestui proiect de mandat, Comisia a subliniat necesitatea existenței unui acord solid privind protecția datelor cu caracter personal ⁽¹⁾.
8. În acest context, AEPD recomandă ca la propunerea actuală să se adauge corelarea cu negocierile purtate cu SUA în legătură cu acest cadru general de protecție a datelor la nivel transatlantic. Ar trebui asigurat faptul că aceste standarde se vor aplica și acordului TFTP II. AEPD recomandă ca această cerință să fie inclusă în acordul actual sau cel puțin să se convină cu guvernul Statelor Unite ca un eventual acord viitor privind protecția datelor să reglementeze schimburile preconizate în cadrul propunerii actuale.
9. În sfârșit, AEPD contribuie activ la pozițiile Grupului de lucru pentru protecția datelor prevăzut la articolul 29 și ale Grupului de lucru pentru poliție și justiție. Pe lângă chestiunile prezentate sau care urmează să fie prezentate în cadrul pozițiilor respective, prezentul aviz analizează propunerea actuală, bazându-se pe observațiile anterioare ale AEPD, atât în legătură cu acordul interimar, cât și cu negocierile cu Statele Unite aflate în desfășurare.

II. ANALIZA PROPUNERII

II.1. Propunerea conține unele îmbunătățiri

10. AEPD recunoaște că această propunere are în vedere anumite îmbunătățiri substanțiale față de acordul interimar TFTP I, precum:
- excluderea datelor SEPA. Propunerea prevede în mod explicit că cererile formulate de către Departamentul de Trezorerie al SUA nu ar trebui să urmărească obținerea niciunei date legate de Zona Unică de Plăți în Euro (articolul 4.2.d);
 - definiția terorismului. Articolul 2 din propunere se bazează pe definiția terorismului în sensul articolului 1 din Directiva-cadru 2002/475/JHA a Consiliului ⁽²⁾.
11. În plus, ca urmare a cererilor formulate de către Parlamentul European și autoritățile europene pentru protecția

datelor, propunerea conține o serie de dispoziții (articolele 14-18) privind drepturile persoanelor vizate, cum ar fi dreptul de a fi informat, dreptul de acces, dreptul la rectificare, ștergere sau blocare, precum și dreptul la aplicarea căilor de atac. Cu toate acestea, aplicabilitatea concretă a acestor dispoziții și a procedurilor ce trebuie urmate de către cetățenii și rezidenții din afara SUA nu sunt clare încă (a se vedea alineatul II.2.3 de mai jos).

II.2. Cu toate acestea, mai sunt necesare și alte îmbunătățiri

12. AEPD împărtășește pe deplin nevoia de a asigura, după cum se are în vedere la articolul 1.1 din propunere, respectarea deplină a vieții private și protecția datelor cu caracter personal. Din această perspectivă, AEPD subliniază că, pentru a îndeplini condițiile cadrului juridic UE privind protecția datelor cu caracter personal, există în continuare unele chestiuni nerezolvate și unele elemente-cheie care necesită îmbunătățiri.

II.2.1. Prelucrarea datelor cu caracter personal avută în vedere este cu adevărat necesară și proporțională?

13. AEPD este pe deplin conștientă de faptul că lupta împotriva terorismului și a finanțării terorismului poate impune anumite restricții în ceea ce privește dreptul la protecția datelor cu caracter personal, precum și în legătură cu dispozițiile privind secretul bancar. Este deja cazul mai multor instrumente UE ⁽³⁾ care conțin o serie de măsuri ce vizează combaterea utilizării ilegale a sistemului financiar în scopul spălării banilor și al finanțării terorismului. Aceste instrumente conțin, de asemenea, dispoziții specifice care permit schimbul de informații cu autorități din țările terțe, precum și garanții pentru protecția datelor cu caracter personal, în conformitate cu Directiva 95/46/CE.
14. În plus, acordul privind asistența juridică reciprocă dintre UE și SUA permite în mod explicit schimbul de informații privind conturile bancare și tranzacțiile financiare între autoritățile de aplicare a legii și prevede condiții și limitări în legătură cu acest schimb. La nivel internațional, de asemenea, așa-numitele Principii Egmont ⁽⁴⁾ au stabilit baza schimbului internațional de informații privind tranzacțiile financiare între Unitățile de informații financiare, stabilind, în același timp, limitările și garanțiile legate de utilizarea datelor care fac obiectul schimbului. În plus, sunt deja în vigoare instrumente pentru schimbul de date între SUA și Eurojust și Eurojust, asigurând în același timp schimbul de informații și protecția datelor cu caracter personal.

⁽¹⁾ A se vedea comunicatul de presă, <http://europa.eu/rapid/pressReleasesAction.do?reference=IP/10/609&format=HTML&aged=0&language=EN&guiLanguage=en>

⁽²⁾ Decizia-cadru a Consiliului din 13 iunie 2002 privind combaterea terorismului, JO L 164, 22.6.2002, p. 3.

⁽³⁾ În special Directiva 2005/60/CE privind prevenirea utilizării sistemului financiar în scopul spălării banilor și finanțării terorismului și Regulamentul (CE) nr. 1781/2006 cu privire la informațiile privind plătitorul care însoțesc transferurile de fonduri.

⁽⁴⁾ <http://www.egmontgroup.org/library/download/5>

15. În acest context, propunerea Comisiei subliniază utilitatea Programului TFTP, astfel cum a fost avansat de către Departamentul de Trezorerie al SUA și de rapoartele înaltului responsabil. Cu toate acestea, condiția prevăzută la articolul 8 din CEDO pentru justificarea imixtiunii în viața privată este mai degrabă o „necesitate” decât o „utilitate”.
16. Conform AEPD, sunt necesare dovezi suficiente în legătură cu valoarea adăugată reală a unui astfel de acord, ținând seama de instrumentele care există deja sau, cu alte cuvinte, în legătură cu măsura în care acordul este cu adevărat necesar pentru a obține rezultate ce nu au fost obținute prin folosirea unor instrumente mai puțin intruzive la adresa vieții private, precum cele prevăzute deja de cadrul comunitar și internațional existent. Conform AEPD, această valoare adăugată ar trebui să fie stabilită fără ambiguități, drept condiție prealabilă pentru încheierea oricărui acord cu SUA privind schimbul de date financiare, precum și având în vedere natura intruzivă a acordului (a se vedea și alineatele 18-22 privind proporționalitatea).
17. AEPD nu este în măsură să aprecieze necesitatea unui astfel de acord. Cu toate acestea, chiar dacă necesitatea acordului este demonstrată, există alte puncte ce merită atenția negociatorilor.
18. Proporționalitatea reprezintă, de asemenea, criteriul principal pentru evaluarea cantității de date cu caracter personal transferate și perioada de stocare a acestora. Articolul 4 din propunere limitează domeniul de aplicare a cererilor SUA. Cu toate acestea, propunerea prevede că datele cu caracter personal vor fi transferate în bloc autorităților din SUA, iar ulterior vor fi păstrate, în principiu, pe o perioadă de 5 ani, indiferent dacă au fost extrase sau dacă există o legătură dovedită cu o anumită investigație sau urmărire penală.

Transferuri în bloc

19. În ciuda cererilor formulate de către Parlamentul European și autoritățile europene pentru protecția datelor, propunerea se bazează în continuare pe conceptul că datele cu caracter personal vor fi transmise în bloc către Departamentul de Trezorerie al SUA. În această privință, este important să se precizeze că, faptul că sistemul SWIFT actual nu permite efectuarea unei căutări specifice nu poate fi considerat o justificare suficientă pentru legalizarea transferurilor în bloc de date conform legislației UE privind protecția datelor.
20. Prin urmare, AEPD consideră că ar trebui găsite soluții care să asigure că transferurile în bloc sunt înlocuite cu mecanisme care permit filtrarea datelor privind tranzacțiile financiare pe teritoriul UE și că doar datele relevante și

necesare sunt transmise către autoritățile din SUA. Dacă aceste soluții nu pot fi găsite imediat, acordul ar trebui în orice caz să definească în mod strict o perioadă de tranziție scurtă după care transferurile în bloc să nu mai fie permise.

Perioada de stocare

21. În ceea ce privește perioada de stocare, AEPD recunoaște faptul că propunerea stabilește în mod corect perioade de stocare maxime, precum și mecanisme care asigură ștergerea datelor cu caracter personal atunci când nu mai sunt necesare. Cu toate acestea, dispozițiile articolului 6 din propunere privind datele neextrase par a fi orientate în direcția opusă. În primul rând, conceptul de „date neextrase” nu este evident în sine și prin urmare ar trebui clarificat. În al doilea rând, motivele pentru care datele neextrase ar trebui păstrate pe o perioadă de 5 ani nu sunt dovedite.
22. AEPD recunoaște pe deplin nevoia de a se asigura accesarea, prelucrarea și păstrarea datelor cu caracter personal necesare pentru o investigație sau urmărire penală împotriva terorismului atâta timp cât este necesar, în unele situații chiar pe o perioadă mai mare de 5 ani, cum este cazul atunci când datele cu caracter personal sunt necesare pentru investigații de lungă durată sau proceduri judiciare. Cu toate acestea, presupunând că datele neextrase sunt date care au fost transferate în bloc și care nu au fost nici accesate, nici folosite pentru o urmărire penală sau o anumită investigație, perioada de stocare permisă pentru păstrarea acestor date trebuie să fie mult limitată. Din această perspectivă, este util să subliniem că Curtea Constituțională Federală Germană a considerat că în cazul păstrării datelor privind telecomunițiile, o perioadă de stocare de 6 luni este deja foarte lungă și prin urmare necesită o justificare corespunzătoare⁽¹⁾. Curtea Constituțională a considerat, se pare, că această perioadă de 6 luni este perioada maximă pentru datele care nu sunt legate de nicio investigație specifică.

II.2.2. Propunerea asigură supraveghere judiciară?

23. Conform mandatului de negociere, o autoritate judiciară publică ar trebui să aibă responsabilitatea de a primi cereri din partea Departamentului de Trezorerie al SUA, de a evalua conformitatea acestora cu acordul și, dacă este cazul, de a solicita furnizorului să transfere datele pe baza unui sistem „push”. Atât Parlamentul European, cât și AEPD au salutat această abordare, care reprezintă o garanție esențială – conform constituțiilor naționale și sistemelor juridice ale statelor membre – pentru a asigura legalitatea și echilibrul transferurilor de date, precum și independența supravegherii.

⁽¹⁾ Hotărârea din 2 martie 2010.

24. Cu toate acestea, propunerea atribuie această sarcină către Europol, o agenție UE pentru prevenirea și combaterea criminalității organizate, a terorismului și a altor forme grave de criminalitate care afectează două sau mai multe state membre ⁽¹⁾. Este evident că Europol nu este o autoritate judiciară.
25. În plus, Europol are interese specifice în ceea ce privește schimbul de date cu caracter personal, în baza acordului propus. Articolul 10 din propunere acordă Europol competența de a solicita informațiile relevante obținute prin TFTP, dacă are un motiv să considere că o persoană sau o entitate are o legătură cu acte de terorism. Este dificil să se găsească o reconciliere între această competență a Europol care ar putea fi importantă pentru îndeplinirea misiunii sale și care impune existența unor relații bune cu Departamentul de Trezorerie al SUA și sarcina Europol de a asigura o supraveghere independentă.
26. În plus, AEPD se întreabă în ce măsură cadrul juridic actual încredințează Europol – în special fără a modifica temeiul său legal conform procedurii ordinare instituite prin Tratatul de la Lisabona – sarcinile și competențele de a face ca o cerere administrativă provenind dintr-o țară terță să fie „obligatorie” (articolul 4.5) pentru o societate privată care astfel „este autorizată și trebuie” să furnizeze date către țara terță respectivă. În acest context, este util să se menționeze faptul că, în stadiul actual al legislației UE, nu este evident dacă o decizie a Europol față de o societate privată ar fi supusă controlului judiciar exercitat de către Curtea Europeană de Justiție.
27. În acest context, AEPD își reiterează poziția conform căreia, în vederea respectării mandatului de negociere și a cadrului juridic actual al UE, sarcina de evaluare a cererilor Departamentului de Trezorerie al SUA ar trebui încredințată unei autorități judiciare publice.

II.2.3. Propunerea conferă drepturi (și protecție) aplicabile subiecților datelor?

28. După cum s-a menționat deja în partea introductivă a prezentului aviz, propunerea enunță o serie de drepturi ale subiecților datelor, cum ar fi dreptul de a fi informat, dreptul de acces, dreptul la rectificare, ștergere sau blocare, precum și dreptul la aplicarea căilor de atac. Prin urmare, este important, pe de o parte, ca unele elemente ale acestor dispoziții să fie îmbunătățite, iar pe de altă parte, să se asigure aplicabilitatea efectivă a acestora.
29. În ceea ce privește dreptul de acces la propriile date cu caracter personal, acordul prevede o serie de limitări. AEPD recunoaște că, în special în contextul combaterii terorismului, pot fi instituite limitări asupra drepturilor subiecților datelor în măsura în care sunt necesare. Cu

toate acestea, propunerea ar trebui să specifice în mod clar că, deși dezvăluirea către o persoană a propriilor date cu caracter personal poate face obiectul unor limitări în împrejurările menționate la articolul 15.2, dezvăluirea acestor informații către autoritățile naționale europene de protecție a datelor ar trebui să fie posibilă în toate cazurile pentru a permite acestora să își îndeplinească eficient sarcina de supraveghere. Desigur, autoritățile de protecție a datelor vor fi supuse unei obligații de confidențialitate în realizarea sarcinilor ce le revin și nu vor dezvălui datele persoanei în cauză, atâta timp cât sunt valabile condițiile de exceptare.

30. În ceea ce privește dreptul la rectificare, la articolul 17.2 se precizează că „Atunci când este posibil, fiecare dintre părți notifică celeilalte părți dacă constată că informații importante pe care i le-a transmis sau le-a primit de la aceasta în temeiul prezentului acord sunt inexacte sau nefiabile”. AEPD consideră că obligația de rectificare a datelor inexacte sau nefiabile reprezintă o garanție fundamentală nu doar pentru subiectul datelor, ci și pentru eficiența acțiunii autorităților de aplicare a legii. Din această perspectivă, autoritățile care fac schimb de date ar trebui să instituie mecanisme care să asigure că această rectificare este întotdeauna fezabilă, și astfel cuvintele „atunci când este posibil” ar trebui să fie eliminate din propunere.
31. Totuși, preocuparea principală a AEPD se referă la aplicabilitatea concretă a acestor drepturi. Pe de o parte, din motive de certitudine și transparență legală, propunerea ar trebui să specifice mai detaliat care sunt procedurile concrete ce ar putea fi folosite de către subiecții datelor pentru a aplica drepturile recunoscute de acord, atât în UE, cât și în SUA.
32. Pe de altă parte, articolul 20.1 precizează în mod explicit și clar că acordul „nu creează și nu conferă niciun drept sau beneficiu niciunei persoane sau entități private sau publice”. AEPD menționează că această dispoziție pare a anula sau cel puțin a pune sub semnul întrebării efectul obligatoriu al acelor dispoziții ale acordului care prevăd drepturi ale subiecților datelor ce nu sunt încă recunoscute și nici aplicabile conform legislației SUA, în special atunci când subiecții datelor nu sunt cetățeni SUA sau rezidenți permanenți. De exemplu, legea SUA privind respectarea vieții private prevede un drept calificat de acces la informațiile cu caracter personal, mai puternic decât dreptul general de acces acordat publicului larg prin Legea SUA privind libertatea informațiilor. Cu toate acestea, Legea SUA privind respectarea vieții private prevede în mod clar că o cerere de acces la dosarul personal este posibilă doar pentru „un cetățean al Statelor Unite sau un cetățean străin căruia i-a fost acceptat dreptul de ședere permanentă” ⁽²⁾.

⁽¹⁾ A se vedea, de exemplu, articolul 3 din Decizia 2009/371/JHA a Consiliului privind înființarea Oficiului European de Poliție (Europol), JO L 121, 15.5.2009, p. 37.

⁽²⁾ Acest lucru este confirmat de informațiile disponibile pe site-ul internet al Departamentului de Trezorerie al SUA „Atunci când formulați o cerere de notificare sau de acces la dosare, trebuie: [...] Să precizați că sunteți cetățean al Statelor Unite sau cetățean străin căruia i-a fost acceptat dreptul de ședere permanentă în Statele Unite; [...]”, <http://www.treas.gov/foia/how-to.html> (ultima accesare la 21 iunie 2010).

33. Prin urmare, AEPD recomandă ca formularea actuală a articolului 20.1 să fie revizuită pentru a garanta că drepturile conferite prin propunere sunt formulate clar și sunt aplicabile inclusiv pe teritoriul SUA.

II.2.4. Propunerea asigură într-o măsură satisfăcătoare supravegherea independentă?

34. Articolul 12 din propunere prevede diferite niveluri de monitorizare a condițiilor și garanțiilor stabilite prin acord. „Supraveghetorii independenți” vor monitoriza în timp real și retrospectiv căutățile înregistrate de către Departamentul de Trezorerie al SUA. În plus, „o persoană independentă numită de Comisia Europeană” va efectua o monitorizare permanentă a primului nivel de supraveghere, inclusiv a independenței acestuia. Ar trebui să se clarifice care vor fi sarcinile acestei persoane independente, cum se va garanta că își poate îndeplini efectiv sarcinile și cui îi este subordonată.

35. Articolul 13 stabilește, de asemenea, un mecanism pentru o revizuire comună, care va fi efectuată după șase luni, iar ulterior la intervale regulate. Această revizuire comună va fi efectuată de către o delegație mixtă UE-SUA, inclusiv pentru reprezentanții delegației UE din partea a două autorități de protecție a datelor, și va avea ca rezultat un raport ce va fi prezentat de către Comisie Parlamentului European și Consiliului.

36. AEPD subliniază că supravegherea independentă reprezintă un element-cheie al dreptului la protecția datelor cu caracter personal, confirmat prin articolul 16 din Tratatul privind funcționarea Uniunii Europene și articolul 8 din Carta drepturilor fundamentale a Uniunii. De curând, Curtea de Justiție a stabilit criterii stricte de independență în Hotărârea sa din 9 martie 2010, Comisia/Germania⁽¹⁾. Este evident că nu pot fi impuse și țărilor terțe același criterii stricte, însă este clar și că o protecție adecvată a datelor cu caracter personal nu poate fi asigurată⁽²⁾ decât în măsura în care există garanții suficiente pentru o supraveghere independentă. Aceasta este, de asemenea, o condiție pentru încheierea acordurilor internaționale cu țările al căror sistem juridic nu stabilește necesitatea controlului de către o autoritate independentă.

37. În acest context, este crucial ca cel puțin modalitățile de supraveghere și de revizuire comună, precum și competențele și garanțiile de independență ale persoanelor implicate în supraveghere să fie definite cu claritate în acord, în loc să fie „coordonate în comun” sau stabilite într-o fază ulterioară de către părți. Este important, în special, să se asigure că atât persoana desemnată de către Comisia Europeană, cât și reprezentanții autorităților europene de protecție a datelor sunt în măsură să acționeze independent și să își îndeplinească efectiv sarcinile de supraveghere.

38. În plus, propunerea nu ar trebui doar să stabilească data primei revizuirii comune, care va avea loc după 6 luni, ci și termenul următoarei revizuirii, care ar putea să fie efectuată ulterior în fiecare an, de exemplu. AEPD recomandă, de asemenea, stabilirea unei corelații între rezultatul acestor revizuirii comune și durata acordului.

39. În acest context, AEPD subliniază că este indicată introducerea unei clauze privind încetarea de drept a efectelor juridice, având în vedere și eventuala disponibilitate a mai multor soluții specifice pe termen mai lung. O clauză privind încetarea de drept a efectelor juridice ar putea reprezenta, de asemenea, un bun stimulent pentru a asigura că se depun eforturile necesare în vederea elaborării acestor soluții, ceea ce ar însemna că nu va mai exista niciun motiv pentru transmiterea în bloc a datelor către Departamentul de Trezorerie al SUA.

40. Pentru a spori eficiența supravegherii și a revizuirii comune, ar trebui să fie disponibile informații și date relevante privind numărul cererilor de acces și de căi de atac, posibila urmărire subsecventă (ștergere, rectificare etc.), precum și numărul deciziilor care limitează drepturile subiecților datelor. În aceeași ordine de idei, în ceea ce privește revizuirea, ar trebuie să fie puse la dispoziție și raportate informații privind cantitatea nu doar de mesaje „accesate” de către Departamentul de Trezorerie al SUA, ci și de mesaje „furnizate” Departamentului de Trezorerie al SUA. Acest lucru ar trebui să fie specificat în acord.

41. În plus, atribuțiile și competențele autorităților europene de protecție a datelor nu ar trebui limitate în niciun fel de această propunere. Din această perspectivă, AEPD menționează că propunerea reprezintă un pas înapoi față de acordul TFTP interimar. Într-adevăr, dacă acordul anterior prevedea în preambul că „prezentul acord nu face nicio derogare de la competențele existente ale autorităților de protecție a datelor din statele membre în materie de protecție a persoanelor în ceea ce privește prelucrarea datelor cu caracter personal ale acestora”, propunerea se referă acum la „supravegherea autorităților competente de protecție a datelor, într-un mod care respectă dispozițiile specifice ale prezentului acord”. Prin urmare, AEPD recomandă ca propunerea să specifice în mod clar că acordul nu constituie o derogare sau limitare a competențelor autorităților europene de protecție a datelor.

III. CONCLUZII

42. AEPD recunoaște că această propunere are în vedere anumite îmbunătățiri substanțiale față de acordul TFTP I interimar, precum excluderea datelor SEPA, o definiție mai limitată a terorismului și mai multe dispoziții detaliate privind drepturile subiecților datelor.

⁽¹⁾ Cauza C-518/07, nepublicată încă în Repertoriu.

⁽²⁾ Articolul 8 din acordul propus prevede că Departamentul de Trezorerie al SUA asigură un nivel de protecție adecvat.

43. Cu toate acestea, AEPD remarcă faptul că ar trebuie să fie îndeplinită o condiție prealabilă esențială pentru evaluarea legitimității unui acord TFTP. Necesitatea schemei trebuie stabilită în legătură cu instrumentele comunitare și internaționale deja existente.
44. În acest caz, AEPD atrage atenția că, pentru îndeplinirea condițiilor cadrului juridic al UE privind protecția datelor cu caracter personal, există în continuare anumite chestiuni nerezolvate și elemente-cheie ce necesită îmbunătățiri, cum ar fi:
- Asigurarea înlocuirii transferurilor în bloc cu mecanisme care să permită filtrarea datelor privind tranzacțiile financiare în interiorul UE și garantarea faptului că doar datele relevante și necesare sunt transmise către autoritățile SUA.
 - Reducerea considerabilă a perioadei de stocare pentru datele neextrase.
 - Atribuirea sarcinii de evaluare a cererilor Departamentului de Trezorerie al SUA unei autorități judiciare publice, conform mandatului de negociere și cadrului juridic actual al UE.
 - Asigurarea faptului că drepturile subiecților datelor conferite prin propunere sunt formulate în mod clar și aplicabile efectiv și pe teritoriul SUA.
 - Sporirea mecanismelor de supraveghere independente, prin:
- (i) asigurarea faptului că sarcinile și rolul atât ale persoanei desemnate de către Comisia Europeană, cât și ale reprezentanților autorităților europene de protecție a datelor sunt definite corespunzător și că aceste persoane sunt în măsură să acționeze independent și să îndeplinească efectiv sarcinile de supraveghere ce le revin;
 - (ii) asigurarea faptului că revizuirile comune au loc în mod regulat și că rezultatul acestora este corelat cu durata acordului prin intermediul unei clauze privind încetarea de drept a efectelor juridice;
 - (iii) extinderea informațiilor disponibile la supraveghetorii independenți și autoritățile de protecție a datelor;
 - (iv) evitarea limitării prin acord a competențelor autorităților europene de protecție a datelor.
- Includerea unei trimiteri la acest aviz în preambulul propunerii.

Adoptat la Bruxelles, 22 iunie 2010.

Peter HUSTINX

Autoritatea Europeană pentru Protecția Datelor