I

(Rezoluții, recomandări și avize)

AVIZE

AUTORITATEA EUROPEANĂ PENTRU PROTECȚIA DATELOR

Avizul Autorității Europene pentru Protecția Datelor referitor la propunerea de decizie-cadru a Consiliului privind utilizarea datelor din registrul cu numele pasagerilor (PNR) în scopul aplicării legii

(2008/C 110/01)

AUTORITATEA EUROPEANĂ PENTRU PROTECȚIA DATELOR,

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

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

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

având în vedere Regulamentul (CE) nr. 45/2001 al Parlamentului European și al Consiliului din 18 decembrie 2000 privind protecția persoanelor fizice cu privire la prelucrarea datelor cu caracter personal de către instituțiile și organele comunitare și privind libera circulație a acestor date [2], în special articolul 41,

având în vedere solicitarea unui aviz primită la 13 noiembrie 2007 din partea Comisiei Europene în conformitate cu articolul 28 alineatul (2) din Regulamentul (CE) nr. 45/2001,

ADOPTĂ PREZENTUL AVIZ

I. INTRODUCERE

Consultarea AEPD

1. Proiectul propunerii de decizie-cadru a Consiliului privind utilizarea datelor din registrul cu numele pasagerilor (PNR) în scopul aplicării legii a fost trimis spre consultare AEPD de către Comisie, în conformitate cu articolul 28 alineatul (2) din Regulamentul (CE) nr. 45/2001 (în continuare „propunerea").

2. Propunerea privește prelucrarea datelor PNR în cadrul Uniunii Europene și este strâns legată de alte mecanisme de colectare și utilizare a datelor pasagerilor, în special de acordul UE-SUA din iulie 2007. Aceste mecanisme prezintă mult interes pentru AEPD, care a avut deja ocazia să trimită câteva comentarii preliminare asupra chestionarului Comisiei privind sistemul PNR al Uniunii Europene prevăzut, trimis în decembrie 2006 părților interesate corespunzătoare [3]. AEPD salută consultarea de către Comisie. În opinia AEPD, preambulul deciziei Consiliului ar trebui să conțină o trimitere la prezentul aviz.

Propunerea și contextul acesteia

3. Scopul propunerii este armonizarea dispozițiilor din statele membre cu privire la obligația transportatorilor aerieni care operează zboruri către sau dinspre teritoriul cel puțin al unui stat membru de a transmite datele PNR către autoritățile competente în scopul prevenirii și combaterii infracțiunilor de terorism și a criminalității organizate.

4. Acorduri pentru transmiterea datelor PNR pentru scopuri comparabile au fost încheiate de către Uniunea Europeană cu Statele Unite ale Americii, precum și cu Canada. Un prim acord încheiat cu Statele Unite ale Americii în mai

[1] JO L 281, 23.11.1995, p. 31.
[2] JO L 8, 12.1.2001, p. 1.

[3] Inclusiv state membre, autorități pentru protecția datelor și asociații ale companiilor aeriene. Acest chestionar a fost elaborat în vederea pregătirii unei evaluări de impact de către Comisia Europeană a propunerii prezentate.

2004 a fost înlocuit printr-un nou acord în iulie 2007 ([1]). Un acord similar a fost încheiat cu Canada în iulie 2005 ([2]). În plus, trebuie să înceapă negocieri între Uniunea Europeană și Australia pentru un acord privind schimbul de date PNR, iar Coreea de Sud solicită, de asemenea, date PNR privind zborurile spre teritoriul acesteia, fără însă a exista, la acest stadiu, un plan de negocieri la nivel european.

5. În cadrul Uniunii Europene, propunerea constituie o completare la Directiva 2004/82/CE a Consiliului ([3]) privind obligația transportatorilor de a comunica date privind pasagerii, cunoscute ca date API, pentru a combate imigrația ilegală și pentru a îmbunătăți controlul la frontiere. Această directivă ar fi trebuia să fie transpusă în dreptul național al statelor membre nu mai târziu de 5 septembrie 2006. Punerea sa în aplicare nu este, totuși, asigurată încă în toate statele membre.

6. Spre deosebire de informațiile prealabile referitoare la pasageri (datele API), care se presupune că ajută la identificarea indivizilor, datele PNR menționate în propunere ar contribui la efectuarea evaluărilor de risc referitoare la persoane, la obținerea de informații și la realizarea de asocieri între persoanele cunoscute și cele necunoscute.

7. Propunerea include următoarele elemente principale:

— Dispune punerea la dispoziție, pentru autoritățile competente din statele membre, de către transportatorii aerieni, a datelor PNR în scopul prevenirii și combaterii infracțiunilor de terorism și a criminalității organizate.

— Prevede desemnarea unei unități de informații despre pasageri (UIP) în fiecare stat membru, în principiu, responsabilă de colectarea datelor PNR de la transportatorii aerieni (sau intermediarii desemnați) și de efectuarea unei analize de risc a pasagerilor.

— Informațiile evaluate în mod corespunzător vor fi transmise autorităților competente din fiecare stat membru. Aceste informații vor face obiectul schimbului cu alte state membre, fiecare caz fiind tratat în mod individual, în scopul menționat anterior.

— Transferul către țările din afara Uniunii Europene este supus unor condiții suplimentare.

— Datele vor fi păstrate timp de treizeci de ani, dintre care opt într-o bază de date pasivă.

— Prelucrarea se va face în conformitate cu (proiectul de) decizie-cadru a Consiliului privind protecția datelor cu caracter personal prelucrate în cadrul cooperării polițienești și judiciare în materie penală (în continuare „decizia-cadru privind protecția datelor") ([4]).

— Un comitet format din reprezentanți ai statelor membre va asista Comisia în ce privește protocolul și aspectele de cifrare, precum și în ce privește criteriile și practica evaluării de risc.

— O evaluare a deciziei trebuie să aibă loc în cel mult trei ani de la intrarea în vigoare a acesteia.

Punctele centrale ale avizului

8. Propunerea pentru care este consultată AEPD constituie un pas suplimentar în tranziția către o colectare de rutină a datelor indivizilor care, în principiu, nu sunt suspectați de nicio infracțiune. După cum s-a menționat anterior, această evoluție are loc la nivel internațional și european.

9. AEDP observă că Grupul de lucru al articolului 29 și Grupul de lucru pentru poliție și justiție au prezentat, de asemenea, un aviz comun privind propunerea ([5]). AEPD sprijină acel aviz. Prezentul aviz evidențiază și dezvoltă un număr de puncte suplimentare.

10. Avizul AEPD va analiza toate aspectele relevante ale propunerii, concentrându-se pe patru probleme principale.

— Prima problemă este cea a legitimității măsurilor prevăzute. Chestiunea scopului, a necesității și a proporționalității propunerii va fi apreciată prin prisma criteriilor de la articolul 8 din Carta drepturilor fundamentale a Uniunii Europene.

— Avizul va analiza, de asemenea, chestiunea dreptului aplicabil operațiunii de prelucrare propuse. În special, merită o atenție specială scopul aplicării deciziei-cadru privind protecția datelor în legătură cu aplicarea primului pilon al legislației privind protecția datelor. Se va analiza, de asemenea, consecința regimului aplicabil de protecție a datelor cu privire la exercitarea drepturilor persoanei vizate.

([1]) Acord între Uniunea Europeană și Statele Unite ale Americii privind prelucrarea și transferul datelor din registrul cu numele pasagerilor (PNR), de către transportatorii aerieni, către Departamentul pentru Securitate Internă al Statelor Unite (DHS) (Acordul PNR 2007) (JO L 204, 4.8.2007, p. 18).

([2]) Acord între Comunitatea Europeană și Guvernul Canadei privind prelucrarea informațiilor prealabile referitoare la pasageri și a datelor din registrul cu numele pasagerilor (JO L 82, 21.3.2006, p. 15).

([3]) Directiva 2004/82/CE a Consiliului din 29 aprilie 2004 privind obligația transportatorilor de a comunica date privind pasagerii (JO L 261, 6.8.2004, p. 24).

([4]) Ultimul proiect al acestei propuneri este disponibil în registrul Consiliului sub numărul 16397/07.

([5]) Aviz comun privind propunerea de decizie-cadru a Consiliului privind utilizarea datelor din registrul cu numele pasagerilor (PNR) în scopul aplicării legii, prezentat de Comisie la 6 noiembrie 2007, adoptat de Grupul de lucru al articolului 29 la 5 decembrie 2007 și de Grupul de lucru pentru poliție și justiție la 18 decembrie 2007, WP 145, WPPJ 01/07.

— În continuare, avizul se va axa pe calitatea destinatarilor datelor la nivel național. În special, calitatea UIP, a intermediarilor și a autorităților competente desemnate să efectueze evaluări ale riscului și să analizeze datele pasagerilor ridică probleme specifice, atât timp cât nu se face nicio precizare în acest sens în propunere.

— A patra problemă este legată de condițiile de transfer al datelor în țările terțe. Nu este clar ce condiții se vor aplica unor astfel de transferuri în cazul în care există diferite categorii de norme: condițiile de transfer în temeiul prezentei propuneri, împreună cu cele din decizia-cadru privind protecția datelor, și acordurile internaționale în vigoare (cu SUA și Canada).

11. Alte puncte substanțiale vor fi identificate în ultima parte, inclusiv evoluțiile pozitive în ce privește protecția datelor, dar și alte motive de îngrijorare pe care le ridică propunerea.

II. LEGITIMITATEA MĂSURILOR PROPUSE

12. Pentru a analiza legitimitatea măsurilor propuse în raport cu principiile fundamentale ale protecției datelor, în special articolul 8 din Carta drepturilor fundamentale a Uniunii Europene și articolele 5 și 8 din Convenția nr. 108 a Consiliului Europei ([1]), este necesară identificarea clară a scopului prelucrării propuse a datelor cu caracter personal, pentru a evalua necesitatea și proporționalitatea acesteia. Trebuie să existe certitudinea că nu există alte mijloace mai puțin agresive care să atingă scopul propus.

Identificarea scopului

13. Formularea propunerii și evaluarea impactului acesteia indică faptul că obiectivul nu este doar de a identifica teroriștii cunoscuți sau infractorii cunoscuți implicați în criminalitatea organizată, prin compararea numelor acestora cu cele incluse în listele administrate de autoritățile de aplicare a legii. Scopul este de a strânge informații cu privire la terorism sau criminalitatea organizată și, mai precis, „efectuarea evaluărilor de risc referitoare la persoane, pentru obținerea de informații și pentru realizarea asocierilor între persoanele cunoscute și cele necunoscute" ([2]). Scopul afirmat la articolul 3 alineatul (5) din propunere este, în primul rând și în același sens, „identificarea persoanelor care sunt *sau pot fi* implicate într-o infracțiune de terorism sau criminalitate organizată, *precum și a persoanelor asociate acestora*".

14. Acesta este motivul invocat pentru a explica faptul că datele API nu sunt suficiente pentru a atinge scopul prezumat. Într-adevăr, după cum s-a menționat anterior, în timp ce datele API ar trebui să ajute la identificarea indivizilor, datele PNR nu au un scop de identificare, ci detaliile din PNR ar contribui la efectuarea evaluărilor de risc referitoare la persoane, obținerea de informații și realizarea asocierilor între persoanele cunoscute și cele necunoscute.

15. Scopul măsurilor avute în vedere nu acoperă numai prinderea persoanelor *cunoscute* ci și localizarea persoanelor care *pot* corespunde criteriilor din propunere.

Pentru a identifica aceste persoane, analizele de risc și identificarea modelelor stau la baza acestui proiect. Considerentul 9 al propunerii afirmă explicit faptul că datele trebuie păstrate „o perioadă de timp suficient de îndelungată pentru a îndeplini scopul elaborării unor indicatori de risc și stabilirii unor modele de deplasare și comportament".

16. Scopul este astfel descris pe două planuri: primul plan constă în obiectivul global de luptă împotriva terorismului și a criminalității organizate, pe când al doilea plan include mijloacele și măsurile inerente atingerii acestui obiectiv. Deși scopul luptei împotriva terorismului și a criminalității organizate pare să fie suficient de clar și de legitim, mijloacele folosite pentru atingerea acestui scop sunt discutabile.

Elaborarea modelelor și a evaluării de risc

17. Propunerea nu dă nicio indicație privind felul în care vor fi elaborate modelele și în care vor fi efectuate evaluările de risc. Evaluarea de impact oferă următoarea precizare în legătură cu felul în care vor fi utilizate datele PNR: se confruntă datele referitoare la pasageri „cu o combinație de caracteristici și modele comportamentale, în vederea obținerii unei evaluări de risc. Atunci când un pasager se încadrează într-o anumită evaluare de risc, acesta ar putea fi identificat ca pasager cu grad mare de risc" ([3]).

18. Persoanele suspectate ar putea fi alese în conformitate cu elemente concrete de suspiciune incluse în datele PNR proprii (de exemplu contactul cu o agenție de turism suspectă, o referire la o carte de credit furată) precum și pe baza „modelelor" sau a unui profil teoretic. Diferite profiluri standard pot fi, într-adevăr, constituite pornind de la modelele de călătorie, pentru „pasageri normali" sau „pasageri suspecți". Aceste profiluri ar permite continuarea investigațiilor în privința acelor pasageri care nu intră în „categoria pasagerilor normali", cu atât mai mult cu cât profilul acestora este asociat cu alte elemente de suspiciune, cum ar fi o carte de credit furată.

19. Cu toate că nu se poate presupune că pasagerii vor fi urmăriți în funcție de religia acestora sau de alte date sensibile, totuși, se pare că aceștia vor face obiectul unor investigații pe baza unui amestec de informații *in concreto* și *in abstracto*, *inclusiv* modele standard și profiluri teoretice.

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

([2]) Expunerea de motive a propunerii, capitolul 1.

([3]) Evaluarea de impact, capitolul 2.1 „Descrierea problemei".

20. Se poate discuta dacă acest tip de investigație poate fi calificat drept profilare. Profilarea ar fi o „metodă computerizată ce folosește extragerea de date dintr-o bază de date și permite sau urmărește să permită clasificarea cu o anumită probabilitate — și astfel cu un anumit grad de eroare — a unui individ într-o categorie anume în scopul de a lua decizii individuale în privința acelei persoane” ([1]).

21. AEPD este conștientă de existența discuțiilor privind definiția profilării. Fie că se recunoaște sau nu în mod oficial că propunerea urmărește *profilarea* pasagerilor, aspectul central în cauză nu îl reprezintă definițiile. Îl reprezintă impactul asupra persoanelor.

22. Principala preocupare a AEPD este legată de faptul că se vor lua decizii în privința persoanelor pe baza modelelor și criteriilor stabilite folosind datele despre pasageri în general. Astfel, s-ar putea lua o decizie cu privire la o persoană, utilizându-se ca referință (cel puțin parțial) modele extrase din datele despre *alte* persoane. Se vor lua, astfel, decizii în legătură cu un context teoretic, fapt ce poate afecta în mare măsură persoanele vizate. Pentru persoane, este foarte dificil să se apere în fața unor astfel de decizii.

23. În plus, evaluarea de risc trebuie să fie efectuată în absența unor standarde uniforme de identificare a suspecților. AEPD consideră că siguranța juridică a întregului proces de filtrare ridică serioase semne de întrebare, considerând că sunt definite într-un mod foarte deficitar criteriile după care fiecare pasager va fi scanat.

24. AEPD reamintește jurisprudența Curții Europene a Drepturilor Omului, în conformitate cu care legea națională trebuie să fie suficient de clară în a indica cetățenilor care sunt circumstanțele și pe ce baze sunt competente autoritățile publice să înregistreze și să utilizeze informații în legătură cu viața lor privată. Informația „trebuie să fie accesibilă persoanei și previzibilă în ceea ce privește efectele”. O normă este „previzibilă” „numai atunci când este redactată cu suficientă precizie, în așa fel încât să permită oricărei persoane — care, la nevoie, poate apela la consultanță de specialitate — să își corecteze conduita” ([2]).

25. În concluzie, în special din cauza acestui tip de riscuri, este necesar ca prezenta propunere să fie analizată cu atenție. Deși scopul general al luptei împotriva terorismului și a criminalității organizate este, în sine, clar și justificat, esența procesului de prelucrare care se va institui nu pare să fie suficient circumscrisă și justificată. Prin urmare, AEPD îndeamnă legiuitorul Uniunii Europene să abordeze fără echivoc acest aspect, înaintea adoptării deciziei-cadru.

Necesitate

26. Caracterul agresiv al măsurilor este evident, după cum s-a arătat anterior. Pe de altă parte, utilitatea acestora nu este nici pe departe demonstrată.

27. Evaluarea de impact asupra propunerii insistă mai mult pe cea mai bună cale de constituire a unui PNR al Uniunii Europene decât pe necesitatea unui astfel de PNR. În evaluare, se face trimitere ([3]) la sistemele PNR existente în alte țări, în special în SUA și în Regatul Unit. Cu toate acestea, este regretabilă lipsa faptelor precise și a cifrelor referitoare la acele sisteme. Sunt raportate „numeroase arestări” cu privire la „diferite infracțiuni” în legătură cu sistemul de semnalizare din UK, fără precizarea unei legături cu terorismul sau cu criminalitatea organizată. Nu sunt date detalii cu privire la programul SUA, cu excepția faptului că „Uniunea Europeană a fost capabilă să evalueze valoarea datelor PNR și să conștientizeze potențialul acestora în scopul aplicării legii”.

28. În plus față de lipsa informațiilor precise *din propunere* privind rezultatele concrete ale unor astfel de sisteme PNR, rapoartele publicate *de alte agenții*, de exemplu GAO în Statele Unite, nu confirmă, la acest stadiu, eficiența măsurilor ([4]).

([1]) Această definiție este extrasă dintr-un studiu recent privind profilarea al Consiliului Europei: *L'application de la Convention 108 au mécanisme de profilage, Eléments de réflexion destinés au travail futur du Comité consultatif (T-PD)*, Jean-Marc Dinant, Christophe Lazaro, Yves Poullet, Nathalie Lefever, Antoinette Rouvroy, noiembrie 2007 (încă nepublicat). A se vedea, de asemenea, definiția dată de Lee Bygrave: „În general, profilarea este procesul de deducere a unui set de caracteristici (tipic comportamentale) ale unei persoane fizice sau entități colective urmată de tratarea acelei persoane/colectivități (sau a altor persoane/colectivități) în lumina acestor caracteristici. În acest sens, profilarea are două componente principale: (i) generarea profilului — procesul de deducere a unui profil; (ii) aplicarea profilului — procesul de tratare a persoanelor/entităților în lumina acestui profil”. L. A. Bygrave, Minding the machine: Article 15 of the EC Data Protection Directive and Automated Profiling, Computer Law & Security Report, 2001, vol. 17, pp. 17-24 http://www.austlii.edu.au/au/journals/PLPR/2000/40.html

([2]) Rotaru împotriva României, nr. 28341/95, alin. (50), (52) și (55). A se vedea, de asemenea, Amann împotriva Elveției, nr. 27798/95, alin. (50) și urm.

([3]) Capitolul 2.1, „Descrierea problemei”.

([4]) A se vedea, de exemplu, raportul Biroului Statelor Unite pentru responsabilitate guvernamentală (GAO) către solicitanții din cadrul Congresului, mai 2007, „Aviation Security: Efforts to Strengthen International Passenger Prescreening are Under Way, but Planning and Implementation Issues remain”, http://www.gao.gov/new.items/d07346.pdf

29. AEPD consideră că tehnica de a evalua riscul prezentat de persoane prin folosirea instrumentelor de extragere de date și a modelelor comportamentale trebuie evaluată în profunzime, iar utilitatea acestora trebuie să fie stabilită fără echivoc în cadrul luptei împotriva terorismului, înainte de a fi utilizate pe o scară atât de largă.

Proporționalitatea

30. Pentru a evalua echilibrul între imixtiune în viața privată a individului și necesitatea măsurii ([1]), sunt luate în considerare următoarele elemente:

— măsurile se aplică tuturor pasagerilor, fie că sunt urmăriți sau nu de către autoritățile de aplicare a legii. Aceasta constituie o căutare anticipativă, la o scară fără precedent,

— deciziile privind persoanele se pot baza pe profiluri teoretice, astfel incluzând o marjă de eroare semnificativă,

— caracterul măsurilor ce trebuie luate împotriva persoanelor ține de aplicarea legii: consecințele în ce privește excluderea sau constrângerea sunt astfel cu mult mai agresive decât în alte contexte, cum ar fi fraudarea cărților de credit sau marketingul.

31. Respectarea principiului proporționalității presupune nu doar eficacitatea măsurii propuse, ci și imposibilitatea de a atinge scopul avut în vedere în propunere prin utilizarea unor instrumente mai puțin agresive în viața privată. Eficacitatea măsurilor avute în vedere nu a fost încă demonstrată. Existența alternativelor trebuie să fie evaluată cu grijă înainte de a pune în practică măsuri noi/suplimentare de prelucrare a informațiilor cu caracter personal. Potrivit AEPD, o astfel de evaluare cuprinzătoare nu a avut încă loc.

32. AEPD dorește să reamintească celălalt sistem la scară largă de monitorizare a deplasării persoanelor în interiorul granițelor Uniunii Europene, operațional sau pe cale de a fi pus în funcțiune, ce include, în special, Sistemul de Informații privind Vizele ([2]) și Sistemul de Informații Schengen ([3]). Deși aceste instrumente nu au drept principal obiectiv lupta împotriva terorismului sau a criminalității organizate, acestea sunt sau vor fi, într-o anumită măsură, accesibile autorităților de aplicare a legii în scopul mai larg de luptă împotriva infracționalității ([4]).

33. Un alt exemplu privește disponibilitatea datelor cu caracter personal incluse în bazele de date ale poliției naționale — în special în ce privește informațiile biometrice — în cadrul Tratatului de la Prüm semnat în mai 2005, care se aplică tuturor statelor membre ale Uniunii Europene ([5]).

34. Toate aceste diferite instrumente au în comun capacitatea de a permite monitorizarea globală a deplasărilor persoanelor, chiar dacă o fac din perspective diferite. Modalitatea în care acestea pot contribui deja la lupta împotriva unor anumite forme de criminalitate, inclusiv a terorismului, ar trebui să facă subiectul unor analize aprofundate și cuprinzătoare, înainte de a decide elaborarea unor noi forme de scanare sistematică a tuturor persoanelor care părăsesc sau intră în Uniunea Europeană cu avionul. AEPD recomandă Comisiei să efectueze o astfel de analiză, ca fiind o etapă necesară în procedura legislativă.

Concluzie

35. În lumina celor menționate, AEPD trage următoarele concluzii în privința legitimității măsurilor propuse. Elaborarea întemeiată pe baze de date fără o privire globală asupra rezultatelor concrete și a neajunsurilor:

— este contrară politicilor legislative raționale în care un nou instrument trebuie adoptat numai după punerea completă în aplicare a celor existente și dovedirea insuficienței acestora ([6]),

— poate avea, de altfel, ca rezultat, o societate de supraveghere totală.

36. Lupta împotriva terorismului poate fi, cu siguranță, un motiv legitim pentru aplicarea excepțiilor la drepturile fundamentale privind viața privată și protecția datelor. Cu toate acestea, pentru a fi valabilă, necesitatea imixtiunii trebuie să fie sprijinită de elemente clare și indubitabile, iar

([1]) În conformitate cu articolul 9 din Convenția 108, „este posibilă derogarea de la dispozițiile prevăzute în articolele 5, 6 și 8 ale prezentei Convenții când o astfel de derogare, prevăzută prin legea Părții, constituie o măsură necesară într-o societate democratică:
1. pentru protejarea securității statului, siguranței publice, intereselor monetare ale statului sau în reprimarea infracțiunilor;
2. pentru a proteja persoanele în cauză sau drepturile și libertățile celorlalți.”.

([2]) Decizia 2004/512/CE a Consiliului din 8 iunie 2004 de instituire a Sistemului de Informații privind Vizele (SIV) (JO L 213, 15.6.2004, p. 5); Propunere de regulament al Parlamentului European și al Consiliului privind Sistemul de Informații privind Vizele (SIV) și schimbul de date între statele membre cu privire la vizele de scurtă ședere, COM(2004) 835 final; Propunere de decizie a Consiliului privind accesul la Sistemul de Informații privind Vizele (SIV) în vederea consultării de către autoritățile statelor membre responsabile cu securitatea internă și de către Europol în scopul prevenirii, detectării și urmăririi infracțiunilor teroriste și a altor fapte penale grave, COM(2005) 600 final.

([3]) A se vedea, în special, Decizia 2007/533/JAI a Consiliului din 12 iunie 2007 privind înființarea, funcționarea și utilizarea Sistemului de Informații Schengen de a doua generație (SIS II) (JO L 205, 7.8.2007).

([4]) A se vedea, cu privire la acest aspect: Avizul Autorității Europene pentru Protecția Datelor privind propunerea de decizie a Consiliului privind accesul la Sistemul de Informații privind Vizele (SIV) în vederea consultării de către autoritățile statelor membre responsabile cu securitatea internă și de către Europol în scopul prevenirii, detectării și urmăririi infracțiunilor teroriste și a altor fapte penale grave [COM(2005) 600 final] (JO C 97, 25.4.2006, p. 6).

([5]) A se vedea avizul AEPD privind deciziile de la Prüm: Avizul din 4 aprilie 2007 privind inițiativa a 15 state membre în vederea adoptării unei decizii a Consiliului privind intensificarea cooperării transfrontaliere, în special în domeniul combaterii terorismului și criminalității transfrontaliere (JO C 169, 21.7.2007, p. 2), și Avizul din 19 decembrie 2007 privind inițiativa Republicii Federale Germania în vederea adoptării unei decizii a Consiliului privind punerea în aplicare a Deciziei 2007/…/JAI privind intensificarea cooperării transfrontaliere, în special în domeniul combaterii terorismului și criminalității transfrontaliere, disponibilă la: http://www.edps.europa.eu

([6]) Acest aspect a fost arătat de mai multe ori de către AEPD, cel mai recent în avizul său din 25 iulie 2007 privind punerea în aplicare a directivei privind protecția datelor (JO C 255, 27.10.2007, p. 1).

proporționalitatea prelucrării trebuie să fie demonstrată. Acest lucru se impune cu atât mai mult în cazul imixtiunii extinse în viața privată a persoanelor, după cum se prevede în propunere.

37. Se poate doar constata faptul că astfel de elemente justificative lipsesc din propunere și că testele privind necesitatea și proporționalitatea nu sunt îndeplinite.

38. AEPD insistă asupra caracterului esențial al testelor privind necesitatea și proporționalitatea, descrise anterior. Acestea reprezintă o *condicio sine qua non* pentru intrarea în vigoare a prezentei propuneri. Orice alt comentariu al AEPD în prezentul aviz trebuie considerat în lumina acestei condiții preliminare.

III. **DREPTUL APLICABIL — EXERCITAREA DREPTURILOR PERSOANELOR VIZATE**

Dreptul aplicabil

39. Analiza ce urmează se va concentra asupra a trei puncte:

— o descriere a diferitelor etape ale prelucrării prevăzute în propunere, în vederea identificării dreptului aplicabil în fiecare stadiu,

— limitele propunerii de decizie-cadru a Consiliului privind protecția datelor cu caracter personal prelucrate în cadrul cooperării polițienești și judiciare în materie penală, în ce privește scopul acesteia și drepturile persoanei vizate,

— o analiză mai generală a gradului în care un instrument din al treilea pilon poate fi aplicat prelucrării datelor actorilor privați în cadrul primului pilon.

Dreptul aplicabil în diferitele etape ale prelucrării

40. Articolul 11 din propunere afirmă că „Statele membre asigură faptul că Decizia-cadru a Consiliului privind protecția datelor cu caracter personal prelucrate în cadrul cooperării polițienești și judiciare în materie penală (…) este aplicabilă prelucrării datelor personale în temeiul prezentei decizii-cadru.”.

41. Cu toate acestea, în ciuda acestei dispoziții, nu este clar în ce măsură decizia-cadru privind protecția datelor — un instrument din cadrul celui de-al treilea pilon al Tratatului UE — se va aplica datelor prelucrate de companiile aeriene, colectate de UIP, iar apoi utilizate de către alte autorități competente.

42. Prima etapă în prelucrarea datelor cu caracter personal prevăzută în propunere este prelucrarea de către companiile aeriene, care sunt obligate să pună datele PNR — folosind, în principiu, o metoda de transmitere „push” — la dispoziția UIP naționale. Din formularea propunerii și din evaluarea de impact ([1]), se pare că datele ar putea fi transmise, de asemenea, în vrac de către companiile aeriene unor intermediari. Companiile aeriene acționează, în principal, într-un mediu comercial, supus legislației naționale de protecție a datelor ce transpune Directiva 95/46/CE ([2]). Problemele privind dreptul aplicabil vor apărea atunci când datele colectate vor fi folosite în scopul aplicării legii ([3]).

43. Datele vor fi apoi filtrate de un intermediar (pentru a fi formatate și pentru a elimina datele PNR care nu sunt incluse pe lista de date solicitate în propunere) sau vor fi trimise direct UIP-urilor. Intermediarii ar putea fi, de asemenea, actori din sectorul privat, cum este cazul SITA, care acționează în acest sens în cadrul Acordului privind PNR încheiat cu Canada.

44. În ce privește UIP, responsabile de evaluarea de risc pentru întreaga cantitate de date, nu este clar cine va fi responsabil de prelucrare. Ar putea fi implicate autoritățile vamale și de frontieră, și nu neapărat autoritățile de aplicare a legii.

45. Transmiterea ulterioară a datelor filtrate către autoritățile „competente” este probabil să aibă loc în contextul aplicării legii. Propunerea menționează că „autoritățile competente includ numai autoritățile însărcinate cu prevenirea sau combaterea infracțiunilor de terorism și criminalității organizate”.

46. Înaintând de-a lungul etapelor prelucrării, actorii implicați și scopul urmărit au o legătură mai strânsă cu cooperarea polițienească și judiciară în materie penală. Cu toate acestea, propunerea nu menționează expres momentul exact de la care se va aplica decizia-cadru privind protecția datelor. Formularea ar induce ideea că se aplică întregii prelucrări, chiar și companiilor aeriene ([4]). Cu toate acestea, decizia-cadru privind protecția datelor cu caracter personal conține câteva limitări.

([1]) Articolul 6.3 din propunere și evaluarea de impact, anexa A, „Metoda de transmitere a datelor de către transportatori”.

([2]) 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).

([3]) A se vedea, în acest sens, consecințele hotărârii PNR. Hotărârea Curții din 30 mai 2006, Parlamentul European/Consiliul (C-317/04) și Comisia (C-318/04), cazurile conexe C-317/04 și C-318/04, Culegere [2006], considerentul 56.

([4]) Articolul 11 din propunere. A se vedea, de asemenea, considerentul 10 din preambul: „Decizia-cadru a Consiliului privind protecția datelor cu caracter personal prelucrate în cadrul cooperării polițienești și judiciare în materie penală (…) ar trebui să fie aplicabilă tuturor datelor prelucrate în conformitate cu prezenta decizie-cadru. Drepturile subiecților datelor în legătură cu prelucrarea acestor date, cum ar fi dreptul la informare, dreptul de acces, dreptul de rectificare, ștergere și blocare, precum și drepturile la compensare și remedii judiciare ar trebui să fie cele prevăzute în decizia-cadru în cauză”.

47. În acest context, AEPD consideră că utilizarea în mod constant a Titlului VI din Tratatul UE drept fundament juridic al obligațiilor legale și în scopul aplicării legii în cazul actorilor din sectorul privat ridică semne de întrebare foarte importante. În plus, este legitimă întrebarea dacă Titlul VI din Tratatul UE poate fi utilizat drept fundament juridic al obligațiilor legale ale autorităților publice care sunt, în principiu, în afara cadrului cooperării în domeniul aplicării legii. Aceste chestiuni vor fi detaliate în continuare în prezentul aviz.

Limitele deciziei-cadru privind protecția datelor

48. Textul propunerii de decizie-cadru a Consiliului privind protecția datelor cu caracter personal prelucrate în cadrul cooperării judiciare și polițienești în materie penală conține cel puțin două limitări care prezintă relevanță pentru domeniul de aplicare al acesteia.

49. În primul rând, scopul deciziei-cadru privind protecția datelor este bine definit chiar în decizia-cadru: se aplică „doar în cazul datelor colectate sau prelucrate de autorități competente, în scopul prevenirii, cercetării, descoperirii sau urmăririi infracțiunilor sau al executării pedepselor” ([1]).

50. În al doilea rând, decizia-cadru privind protecția datelor nu ar trebui să se aplice prelucrării datelor efectuate doar la nivel național, ci se limitează la schimbul de date între statele membre și la transferul ulterior în țările terțe ([2]).

51. Decizia-cadru privind protecția datelor prezintă, de asemenea, anumite regrese în raport cu Directiva 95/46/CE, în special o largă excepție la principiul limitării scopului. În ce privește acest principiu, propunerea limitează în mod clar scopul prelucrării la lupta împotriva terorismului și a criminalității organizate. Cu toate acestea, decizia-cadru privind protecția datelor permite prelucrarea în scopuri mai largi. Într-un astfel de caz, *lex specialis* (propunerea) ar trebui să prevaleze asupra *lex generalis* (decizia-cadru privind protecția datelor) ([3]). Acest aspect trebuie menționat în mod expres în textul propunerii.

52. Din acest motiv, AEPD recomandă adăugarea următoarei dispoziții la propunere: „Datele cu caracter personal transmise de companiile aeriene în conformitate cu decizia-cadru nu pot fi prelucrate în alte scopuri decât lupta împotriva terorismului și a criminalității organizate. Excepțiile prevăzute cu privire la principiul scopului în Decizia-cadru a Consiliului privind protecția datelor cu caracter personal prelucrate în cadrul cooperării polițienești și judiciare în materie penală nu se aplică”.

53. În concluzie, AEPD constată o deficiență serioasă de siguranță juridică în privința regimului protecției datelor aplicabil diferiților actori implicați în proiect, în special companiilor aeriene și altor actori din cadrul primului pilon: fie că este vorba de normele din propunere, de normele din decizia-cadru privind protecția datelor sau de legislația națională care transpune Directiva 95/46/CE. Legiuitorul ar trebui să indice cu claritate în ce moment exact al prelucrării se aplică aceste diverse norme.

Condițiile aplicării normelor din cadrul primului și celui de-al treilea pilon

54. AEPD consideră că faptul că un instrument din cadrul celui de-al treilea pilon creează în mod constant obligații legale în scopul aplicării legii în cazul actorilor din sectorul privat sau public și care sunt, în principiu, în afara cadrului cooperării în domeniul aplicării legii ridică semne de întrebare foarte importante.

55. În acest caz, se poate face o comparație cu alte două cazuri în care sectorul privat a fost implicat în păstrarea și transferul datelor în vederea aplicării legii:

— *Cazul PNR-SUA în care s-a prevăzut transferul sistematic al datelor PNR de către companiile aeriene către autoritățile de aplicare a legii:* Hotărârea Curții de Justiție în cazul PNR a scos încheierea acordului PNR din atribuțiile Comunității. Unul dintre motive a fost că transferul datelor PNR către US CBP constituie operații de prelucrare care țin de securitatea publică și de activități ale statului în domeniul dreptului penal ([4]). În acest caz, operația de prelucrare consta într-un transfer către CBP *în mod sistematic*, element prin care se diferențiază de cazul următor:

— *Păstrarea generală a datelor de către operatorii de comunicații electronice*. În ce privește atribuțiile Comunității de a stabili un astfel de termen de păstrare, se poate constata o diferență față de cazul PNR-SUA, considerând că Directiva 2006/24/CE ([5]) prevede doar o obligație de păstrare, datele rămânând sub controlul operatorilor. Nu se are în vedere niciun transfer sistematic de date către autoritățile de aplicare a legii. Se poate concluziona că, atât timp cât datele rămân sub controlul prestatorilor de servicii, respectivii prestatori rămân, de asemenea, răspunzători de respectarea obligațiilor de protecție a datelor cu caracter personal față de persoanele vizate.

([1]) Considerentul 5(a), versiunea din 11 decembrie 2007 a deciziei-cadru privind protecția datelor.

([2]) Articolul 1.

([3]) Referitor la acest punct, ar trebui analizat și discutat cu atenție textul articolului 27b din ultimul proiect al deciziei-cadru privind protecția datelor în cadrul celui de-al treilea pilon.

([4]) Hotărârea Curții din 30 mai 2006, Parlamentul European/Consiliul (C-317/04) și Comisia (C-318/04), cazurile conexe C-317/04 și C-318/04, Culegere [2006], considerentul 56.

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

56. În prezenta propunere a Uniunii Europene referitoare la PNR, companiile aeriene trebuie să pună la dispoziție în mod sistematic datele PNR ale tuturor pasagerilor. Cu toate acestea, aceste date nu sunt transferate direct, în vrac, către autoritățile de aplicare a legii: acestea pot fi trimise unui intermediar și sunt evaluate de o terță parte, al cărei statut rămâne neclar, înainte ca informațiile alese să fie trimise autorităților competente.

57. Partea principală a prelucrării are loc într-o zonă gri, având legături strânse atât cu primul cât și cu al treilea pilon. După cum se va detalia în capitolul IV, calitatea actorilor implicați în prelucrarea datelor nu este clară. Companiile aeriene nu sunt, în mod cert, autorități de aplicare a legii, iar intermediarii pot fi actori din sectorul privat. Chiar și în ce privește UIP, care ar fi autorități publice, trebuie subliniat faptul că nu orice autoritate publică are calitatea și atribuțiile de a îndeplini activități de aplicare a legii în mod constant.

58. 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, fapt ce ridică problema cadrului de protecție a datelor (primul sau al treilea pilon) care se aplică condițiilor acestei cooperări: ar trebui ca normele să se întemeieze pe calitatea operatorului de date (sectorul privat) sau pe scopul urmărit (aplicarea legii)?

59. AEPD a reamintit deja riscul unei lacune în legislație în cazul activităților ce țin de primul și al treilea pilon ([1]). Nu este, într-adevăr, deloc clar dacă măsurile întreprinderilor private, legate într-un fel cu aplicarea dreptului penal, intră în sfera de acțiune a legiuitorului Uniunii Europene în conformitate cu articolele 30, 31 și 34 din Tratatul UE.

60. În cazul în care cadrul general (primul pilon) nu s-ar aplica, un prestator de servicii ar trebui să facă distincții dificile în cadrul proprii baze de date. În cadrul regimului actual, este limpede că operatorul de date trebuie să respecte în aceeași măsură protecția datelor față de persoanele vizate fără deosebire de scopul care justifică păstrarea datelor. Trebuie, în aceste condiții, să nu se ajungă la situația în care prelucrarea de către prestatorii de servicii în diferite scopuri să fie supusă unor cadre diferite de protecție a datelor.

([1]) A se vedea avizul Autorității Europene pentru Protecția Datelor privind comunicarea Comisiei către Parlamentul European și Consiliu cu privire la continuarea programului de lucru pentru o mai bună punere în aplicare a directivei privind protecția datelor (JO C 255, 27.10.2007, p. 1). A se vedea, de asemenea, Raportul anual 2006, p. 47.

Exercitarea drepturilor persoanelor vizate

61. Diferitele regimuri juridice care s-ar aplica la nivel național ar avea un impact major, în primul rând, asupra exercitării drepturilor de către persoana vizată.

62. Se afirmă în preambulul propunerii că „dreptul la informare, dreptul de acces, dreptul de rectificare, ștergere și blocare, precum și drepturile la compensare și remedii judiciare ar trebui să fie cele prevăzute în decizia-cadru în cauză". Cu toate acestea, această afirmație nu răspunde la întrebarea privind identitatea operatorului însărcinat să răspundă solicitărilor persoanelor vizate.

63. Informațiile privind prelucrarea pot fi comunicate de către companiile aeriene, dar situația este mai complexă când este vorba de accesul la date sau rectificarea acestora. Aceste drepturi sunt, într-adevăr, restrânse prin decizia-cadru privind protecția datelor. După cum s-a menționat anterior, posibilitatea de a obliga un prestator de servicii cum este o companie aeriană să acorde drept de acces și de rectificare diferențiat cu privire la datele pe care le deține, în funcție de scopul urmărit (comercial sau privind aplicarea legii), este îndoielnică. Se poate argumenta că aceste drepturi trebuie să fie exercitate în fața UIP sau a altor autorități competente desemnate. Cu toate acestea, propunerea nu mai dă alte indicații în acest sens și, după cum s-a menționat deja, nu este clar nici faptul că aceste autorități (cel puțin UIP) vor fi autorități de aplicare a legii deținătoare, în mod normal, ale unor proceduri de acces restricționat (posibil indirect).

64. Persoana riscă, de asemenea, să se confrunte cu diferiți destinatari ai datelor, cel puțin în ce privește UIP: datele sunt, într-adevăr, transmise UIP din țara de plecare/sosire a zborurilor, dar posibil și UIP-urilor din alte state membre, după caz. Mai mult, este posibil ca mai multe state membre să înființeze sau să desemneze o UIP unică și comună. Persoana vizată poate, în acest caz, să își exercite drepturile în fața unei autorități din alt stat membru. Din nou, nu este clar dacă normele naționale de protecție a datelor se vor aplica (se presupune că acestea sunt armonizate în cadrul Uniunii Europene), sau dacă va trebui luată în calcul legislația specifică de aplicare a legii (dată fiind lipsa unei armonizări totale la nivel național în cadrul celui de-al treilea pilon).

65. Aceeași problemă există în privința accesului la datele prelucrate de intermediari, al căror statut este neclar, și care ar putea fi comun cu cel la companiilor aeriene în diferite state ale Uniunii Europene.

66. AEPD regretă incertitudinea care persistă cu privire la exercitarea acestor drepturi fundamentale ale persoanei vizate. Aceasta subliniază faptul că situația se datorează, în principal, faptului că actorilor care nu au, ca activitate principală, aplicarea legii li se încredințează astfel de responsabilități.

Concluzie

67. AEPD consideră că propunerea ar trebui să clarifice aspectul regimului juridic aplicabil fiecărui stadiu al prelucrării, și să specifice în fața cărui actor sau autoritate trebuie exercitat dreptul la acces sau calea de atac. AEPD reamintește că, în conformitate cu articolul 30 alineatul (1) litera (b) din Tratatul UE, dispozițiile privind protecția datelor ar trebui să corespundă și să acopere întreaga gamă a operațiilor de prelucrare stabilite în propunere. O simplă trimitere la decizia-cadru privind protecția datelor nu este suficientă, dat fiind domeniul de aplicare limitat al deciziei-cadru și limitările de drepturi pe care le conține. În privința autorităților de aplicare a legii, normele din decizia-cadru privind protecția datelor ar trebui să se aplice, cel puțin, întregii prelucrări prevăzute în propunere, pentru a garanta coerența aplicării principiilor de protecție a datelor.

IV. CALITATEA DESTINATARILOR

68. AEPD constată că propunerea nu prezintă nicio indicație cu privire la calitatea destinatarilor datelor cu caracter personal colectate de companiile aeriene, fie că e vorba de intermediari, unități de informații despre pasageri sau autorități competente. Trebuie subliniat raportul direct dintre calitatea destinatarului și tipul de garanții privind protecția datelor aplicabile acelui destinatar. Diferența dintre garanțiile asigurate, în special, de normele primului și ale celui de-treilea pilon au fost deja menționate. Este esențial ca regimul aplicabil să fie clar pentru toți actorii implicați, inclusiv pentru guvernele naționale, organismele de aplicare a legii, autoritățile de protecție a datelor, precum și pentru operatorii de date și persoanele vizate implicate.

Intermediari

69. În propunere, nu se dă nicio indicație cu privire la calitatea intermediarilor ([1]). Rolul intermediarilor, de a opera sau a prelucra datele, nu este, de asemenea, specificat. Din experiență, se pare că sarcina de a strânge datele PNR direct de la companiile aeriene pentru a le transmite UIP ar putea fi încredințată unei entități din sectorul privat, care poate fi un sistem informatic de rezervare sau o altă entitate. Acesta este modul în care sunt prelucrate datele în cadrul Acordului privind PNR cu Canada. SITA ([2]) este întreprinderea responsabilă cu prelucrarea informațiilor. Rolul intermediarului este hotărâtor, deoarece acesta ar putea fi răspunzător de eliminarea/reformatarea datelor care sunt transmise companiilor aeriene în vrac ([3]). Chiar dacă intermediarii sunt obligați să anuleze informațiile prelucrate odată ce au fost transferate UIP, prelucrarea în sine este foarte delicată: o consecință a intervenției intermediarilor este crearea unei baze de date suplimentare conținând cantități uriașe de date, inclusiv, potrivit propunerii, date sensibile (intermediarii fiind obligați să șteargă acele date sensibile). Din aceste motive, AEPD recomandă să nu fie implicați intermediari în prelucrarea datelor pasagerilor, cu excepția cazului în care calitatea și sarcinile intermediarilor sunt strict specificate.

Unitățile de informații despre pasageri

70. UIP au un rol hotărâtor în identificarea persoanelor care sunt sau ar putea fi implicate în infracțiuni de terorism sau criminalitate organizată sau asociate la acestea. În conformitate cu propunerea, acestea răspund de crearea indicatorilor de risc și de furnizarea informațiilor privind modelele de călătorie ([4]). În cazul în care evaluarea de risc se bazează pe modele de călătorie standardizate și nu pe elemente de probă materiale legate de un caz concret, analiza poate fi considerată ca fiind o anchetă anticipativă. AEPD insistă asupra faptului că acest tip de prelucrare este, în principiu, strict reglementat în legislația statelor membre (dacă nu chiar interzis), și intră în atribuțiile unor autorități publice specifice a căror funcționare este, de asemenea, strict reglementată.

71. UIP sunt, astfel, însărcinate cu operațiuni foarte sensibile de prelucrare a informațiilor, fără ca propunerea să dea detalii despre calitatea și condițiile în care și-ar exercita atribuțiile aceste unități. Cu toate că este probabil ca această sarcină să fie îndeplinită de un organism guvernamental, posibil vama sau controlul la frontieră, propunerea nu împiedică explicit statele membre de a încredința această activitate serviciilor de informații sau oricărui alt tip de organism de prelucrare. AEPD subliniază faptul că transparența și garanțiile aplicate serviciilor de informații nu sunt întotdeauna identice celor aplicabile autorităților tradiționale de aplicare a legii. Detaliile privind calitatea UIP sunt hotărâtoare, deoarece aceasta va avea consecințe directe asupra cadrului legal aplicabil și a condițiilor de supraveghere. AEPD consideră că propunerea trebuie să includă o dispoziție suplimentară care să detalieze caracteristicile UIP.

([1]) Articolul 6 din propunere.

([2]) SITA a fost creată în 1949 de 11 membri companii aeriene. Soluții cu valoare adăugată sunt prestate industriei de transport aerian prin întreprinderea comercială SITA INC (servicii informatice și de rețelistică) și servicii de rețele de comunicații prin SITA SC pe bază de cooperare.

([3]) Evaluarea de impact, anexa A, „Metode de transmitere a datelor de către transportatori".

([4]) Articolul 3 din propunere.

Autoritățile competente

72. Articolul 4 din propunere sugerează că orice autoritate responsabilă de prevenirea și combaterea infracțiunilor de terorism și crimă organizată poate primi datele. Scopul este clar definit, dar calitatea autorității lipsește. Propunerea nu prevede nicio limitare a destinatarilor la autoritățile de aplicare a legii.

După cum s-a menționat anterior referitor la UIP, este hotărâtor ca informațiile sensibile în cauză să fie prelucrate într-un mediu cu un cadru legal clar. Este mai curând cazul, de exemplu, al autorităților de aplicare a legii decât cel al serviciilor de informații. Luând în considerare datele extrase și cercetarea anticipativă inclusă în propunere, nu se poate elimina posibilitatea implicării unor astfel de servicii de informații în prelucrarea datelor fără a exclude alte categorii de autorități.

Concluzie

73. În general, AEPD constată că aplicarea unui sistem PNR în Uniunea Europeană devine cu atât mai dificilă cu cât autoritățile de aplicare a legii au atribuții diferite în funcție de dreptul național al statelor membre, incluzând sau nu domeniul informațiilor, cel fiscal, al imigrației sau al poliției. Acesta este, totuși, un motiv în plus pentru a recomanda ca propunerea să fie mult mai precisă cu privire la calitatea actorilor menționați și la garanțiile privind controlul îndeplinirii sarcinilor acestora. Ar trebui să fie introduse dispoziții suplimentare în propunere pentru a specifica în mod strict atribuțiile și obligațiile legale ale intermediarilor, ale UIP și ale altor autorități competente.

V. CONDIȚII PENTRU TRANSFERUL ÎN ȚĂRILE TERȚE

74. Propunerea prevede anumite garanții în legătură cu transferul datelor PNR în țările terțe ([1]). În special, aceasta prevede explicit aplicarea deciziei-cadru privind protecția datelor în cazul transferului de date, prevede o limitare specifică a scopului și afirmă necesitatea consimțământului statului membru în cazul transferului ulterior. Transferul ar trebui să respecte, de asemenea, legislația națională a statului membru respectiv, precum și orice acord internațional aplicabil.

75. Multe semne de întrebare rămân, totuși, în special cu privire la calitatea consimțământului, condițiile de aplicare a deciziei-cadru privind protecția datelor și problema „reciprocității" în transmiterea datelor către țări terțe.

([1]) Articolul 8 din propunere.

Calitatea consimțământului

76. Statul membru originar trebuie să își dea consimțământul expres pentru transferul ulterior de la o țară terță la o altă țară terță. Propunerea nu precizează în ce condiții și prin cine se va da acest consimțământ, și dacă autoritățile naționale însărcinate cu protecția datelor trebuie implicate în decizie. AEPD consideră că modalitatea de transmitere a consimțământului trebuie să fie, cel puțin, în conformitate cu legile naționale care precizează condițiile pentru transferul datelor cu caracter personal în țările terțe.

77. În plus, consimțământul statului membru nu ar trebui să prevaleze asupra principiului potrivit căruia trebuie prevăzut un nivel adecvat de protecție de către statul destinatar pentru prelucrarea planificată. Aceste condiții ar trebui să fie cumulative, la fel ca în decizia-cadru privind protecția datelor (articolul 14). Astfel, AEPD sugerează introducerea unei litere (c) la alineatul (1) din articolul 8 după cum urmează: „și (c) țara terță asigură un nivel adecvat de protecție pentru prelucrarea de date planificată". AEPD reamintește, în acest sens, că trebuie instituite mecanisme de asigurare a unor standarde comune și a unor decizii coordonate cu privire la asigurarea unui nivel adecvat de protecție ([2]).

Aplicarea deciziei-cadru privind protecția datelor

78. Propunerea face trimitere la condițiile și garanțiile menționate de decizia-cadru privind protecția datelor, specificând, de asemenea, în mod explicit, anumite condiții, în special consimțământul statului membru respectiv, menționat anterior, și limitarea scopului la prevenirea și lupta împotriva infracțiunilor de terorism și criminalitate organizată.

79. Decizia-cadru privind protecția datelor prevede condiții pentru transferul datelor cu caracter personal în țările terțe, și anume în ceea ce privește limitarea scopului, calitatea destinatarilor, consimțământul statului membru și principiul adecvării. Cu toate acestea, aceasta prevede, de asemenea, derogări de la condițiile de transfer menționate: interese legitime mai importante, în special interese publice importante, pot reprezenta un temei suficient pentru transfer, chiar dacă condițiile menționate anterior nu sunt îndeplinite.

80. După cum s-a menționat anterior, la capitolul III din prezentul aviz, AEPD consideră că trebuie să se precizeze clar în textul propunerii faptul că garanțiile mai precise din propunere prevalează asupra condițiilor — și excepțiilor — generale din decizia-cadru privind protecția datelor, atunci când aceasta se aplică.

([2]) Avizul AEPD din 26 iunie 2007 privind propunerea de decizie-cadru a Consiliului privind protecția datelor cu caracter personal prelucrate în cadrul cooperării polițienești și judiciare în materie penală, punctele 27-30 (JO C 139, 23.6.2007, p. 1).

Reciprocitate

81. Propunerea abordează aspectul posibilelor „solicitări vindicative" ale țărilor care ar putea cere Uniunii Europene date PNR pentru zboruri din Uniunea Europeană spre teritoriul acestora. În cazul în care Uniunea Europeană solicită date din bazele de date ale companiilor aeriene ale unor astfel de țări terțe, pe motiv că operează zboruri către sau din UE, astfel de țări terțe ar putea cere același lucru de la companiile aeriene din UE, inclusiv date ale cetățenilor UE. Deși Comisia consideră această eventualitate ca fiind „foarte îndepărtată", prevede o astfel de posibilitate. Propunerea arată, în această privință, faptul că acordul cu SUA și Canada prevede un astfel de tratament reciproc „care poate fi pus în aplicare în mod automat" ([1]). AEPD consideră că semnificația unei astfel de reciprocități automate și aplicarea garanțiilor unor astfel de transferuri ridică semne de întrebare, în special luând în calcul existența unui nivel adecvat de protecție în țara respectivă.

82. Ar trebui să se facă distincția între țări terțe care au încheiat deja un acord cu Uniunea Europeană, și acele țări care nu au încheiat un astfel de acord.

Țări care nu au încheiat un acord cu Uniunea Europeană

83. AEPD constată că reciprocitatea ar putea duce la transferul datelor cu caracter personal către țări în care nu pot fi asigurate garanții în privința standardelor democratice și a unui nivel adecvat de protecție a datelor.

84. Evaluarea de impact oferă elemente suplimentare cu privire la condițiile de transfer al datelor către țările terțe: se evidențiază avantajul sistemului PNR-UE, în care datele sunt filtrate de UIP. Transferul către autoritățile competente ale statelor membre și, probabil, și către țările terțe ([2]) ar privi doar anumite date despre persoanele suspecte (și nu date în vrac). AEPD recomandă clarificarea acestui punct în textul propunerii. O simplă declarație în evaluarea de impact nu asigură protecția necesară.

85. Selectarea datelor contribuie la minimizarea impactului asupra vieții private a pasagerilor, dar trebuie reamintit faptul că principiile privind protecția datelor nu se limitează la reducerea cantității de date colectate, și includ principii cum ar fi necesitatea, transparența și exercițiul drepturilor persoanelor vizate, toate principiile trebuind luate în calcul pentru a determina dacă o țară terță oferă un nivel adecvat de protecție.

Țări care au încheiat un acord bilateral cu Uniunea Europeană

86. Evaluarea de impact arată faptul că o astfel de prelucrare va oferi Uniunii Europene posibilitatea „de a insista asupra anumitor standarde și de a asigura o coerență în astfel de acorduri bilaterale cu țări terțe. Aceasta va oferi, de asemenea, posibilitatea de a solicita tratament reciproc țărilor terțe cu care Uniunea Europeană a încheiat un acord, ceea ce nu este posibil în acest moment" ([3]).

87. Din aceste observații reiese problema impactului propunerii asupra acordurilor în vigoare cu Canada și SUA. Condițiile pentru accesarea datelor din aceste acorduri sunt, într-adevăr, mult mai largi, deoarece nu sunt supuse unei selecții asemănătoare înainte de a fi transferate în acele țări terțe.

88. Evaluarea de impact arată că „în cazul în care Uniunea Europeană a încheiat un acord internațional cu o țară terță pentru schimbul/transmiterea datelor PNR unei astfel de țări terțe, acordul respectiv va fi luat în considerare în mod corespunzător. Transportatorii ar trebui să trimită datele PNR către unitățile de informații despre pasageri în conformitate cu practicile normale potrivit măsurii curente. UIP care recepționează astfel de date le transmit autorității competente din țara terță cu care s-a încheiat un astfel de acord" ([4]).

89. Deși, pe de o parte, propunerea pare să vizeze transferul *doar* al datelor *selectate* către oricare autoritate competentă, fie în Uniunea Europeană, fie în afara acesteia, pe de altă parte, evaluarea de impact, preambulul propunerii (considerentul 21) și articolul 11 reamintesc faptul că acordurile existente ar trebui luate în considerare în mod corespunzător. Aceasta poate conduce la concluzia că filtrarea poate fi o măsură valabilă doar în cazul acordurilor ce vor fi încheiate în viitor. Se poate preconiza, în acest sens, că accesul nediferențiat va fi, în continuare, modelul de acces, de exemplu al datelor PNR de către autoritățile SUA, în conformitate cu dispozițiile acordului UE-SUA, dar că, în paralel și de la caz la caz, un transfer de date către SUA ar putea interveni, referitor la date specifice identificate de UIP, inclusiv dar fără să se limiteze la date privind zborurile către SUA.

90. AEPD regretă lipsa clarității cu privire al acest punct hotărâtor din propunere. Aceasta consideră de maximă importanță coerența condițiilor pentru transferul datelor PNR către țări terțe și conformitatea acestora cu un nivel armonizat de protecție. În plus, din motive de siguranță juridică, ar trebui incluse în propunere, și nu doar în evaluarea de impact, cum este cazul în acest moment, precizări cu privire la garanțiile aplicate transferului de date.

([1]) Expunerea de motive a propunerii, capitolul 2.
([2]) Evaluarea de impact, capitolul 5.2, „Protecția vieții private".
([3]) Evaluarea de impact, capitolul 5.2, „Relațiile cu țările terțe".
([4]) Evaluarea de impact, anexa A, „Organisme care recepționează date de la unitățile de informații despre pasageri".

VI. **ALTE ASPECTE IMPORTANTE**

Prelucrarea automată

91. AEPD constată că propunerea exclude în mod explicit posibilitatea ca o măsură de aplicare să fie întreprinsă de unitățile de informații despre pasageri și de autoritățile competente ale statelor membre numai pe baza prelucrării automate a datelor PNR sau pe baza rasei sau originii etnice, a convingerilor religioase sau filozofice, a opiniilor politice sau a orientării sexuale ale unei persoane ([1]).

92. O astfel de precizare este binevenită întrucât reduce riscul măsurilor arbitrare împotriva persoanelor. Cu toate acestea, AEPD constată că domeniul de aplicare al acesteia este limitat la *măsuri de aplicare* ale UIP sau ale autorităților competente. Aceasta nu exclude, în actuala formulare, filtrarea automată a persoanelor în conformitate cu profiluri standard, nici nu împiedică constituirea automată a listelor persoanelor suspectate și luarea unor măsuri cum ar fi supravegherea extinsă, atât timp cât aceste măsuri nu sunt considerate măsuri de aplicare.

93. AEPD consideră că noțiunea de *măsură de aplicare* este prea vagă, și că, în principiu, *nicio decizie* nu ar trebui luată cu privire la persoane *doar* în baza prelucrării automate a datelor ([2]). AEPD recomandă modificarea textului în mod corespunzător.

Calitatea datelor

94. Propunerea conține, la articolul 5 alineatul (2), o precizare importantă prin aceea că stabilește în mod clar faptul că nicio obligație nu este instituită în sarcina companiilor aeriene de a colecta sau păstra date suplimentare față de cele colectate în scopul comercial inițial.

95. Câteva aspecte ale prelucrării acestor date merită, totuși, un comentariu suplimentar:

— Datele care trebuie puse la dispoziție, astfel cum sunt enumerate în anexa 1 din propunere, acoperă un domeniu foarte larg, iar lista este asemănătoare listei de date disponibile pentru autoritățile SUA din acordul UE-SUA. Calitatea câtorva dintre datele solicitate a fost deja pusă la îndoială în diferite ocazii de către autoritățile de protecție a datelor, și în special de către Grupul de lucru Articolul 29 ([3]).

— Din formularea evaluării de impact ([4]) și din articolul 6.3 din propunere, ar reieși că datele ar putea fi transmise, de asemenea, în vrac de către companiile aeriene unor intermediari. Într-o primă etapă, datele transmise unei terț nu ar fi nici măcar limitate în conformitate cu datele PNR enumerate în anexa 1 din propunere.

— În ce privește prelucrarea datelor sensibile, chiar dacă aceste date ar putea fi eliminate în etapa intermediarilor, rămâne un semn de întrebare privind stricta necesitate a transferului câmpului liber de către companiile aeriene.

AEPD sprijină pozițiile susținute în avizul Grupului de lucru al Articolului 29 în acest sens.

Metoda de transfer a datelor PNR

96. Transportatorii aerieni stabiliți în afara Uniunii Europene sunt solicitați să *înainteze* datele (metoda „*push*") către UIP sau către intermediari atât timp cât aceștia dețin infrastructura tehnică necesară. Dacă această condiție nu este îndeplinită, va trebui ca aceștia să permită extragerea datelor prin metoda „*pull*".

97. Îngăduirea unor metode diferite de comunicare a datelor în funcție de fiecare companie aeriană nu va face altceva decât să genereze mai multe dificultăți cu privire la controlul respectării normelor de protecție a datelor în cadrul transferului datelor PNR. Astfel se riscă, de asemenea, perturbarea concurenței dintre companiile aeriene din interiorul și din exteriorul Uniunii Europene.

98. AEPD reamintește faptul că metoda „*push*", care permite companiilor aeriene să păstreze controlul asupra calității datelor transferate și a circumstanțelor transferului, este singura metodă admisibilă în ce privește proporționalitatea prelucrării. Mai mult, aceasta trebuie să constea într-o operațiune de „*push*" efectiv, adică datele nu ar trebui să fie trimise în vrac unui intermediar, ci filtrate chiar din prima etapă a prelucrării. nu este admisibil ca datele inutile — și datele care nu sunt incluse în anexa 1 din propunere — să fie trimise unei terțe părți, chiar dacă acele date vor fi șterse imediat de către această terță parte.

Păstrarea datelor

99. Articolul 9 din propunere prevede un termen de păstrare a datelor PNR de 5 ani, cu o perioadă suplimentară de 8 ani în care datele trebuie să fie păstrate într-o bază de date „pasivă" care va fi accesibilă în condiții stricte.

([1]) Considerentul 20 și articolul 3 alineatele (3) și (5) din propunere.

([2]) A se vedea, în acest sens, articolul 15 alineatul (1) din Directiva 95/46/CE. Directiva interzice astfel de decizii automate în cazurile în care individul ar fi afectat de decizie. În ce privește contextul propunerii, deciziile luate în cadrul aplicării legii sunt susceptibile, în orice caz, de a afecta grav persoanele vizate. De asemenea, faptul de a fi supus unor verificări ulterioare poate afecta persoana vizată, mai ales dacă aceste măsuri sunt luate în mod repetat.

([3]) A se vedea, în special, Avizul nr. 5/2007 din 17 august 2007 privind evaluarea acordului între Uniunea Europeană și Statele Unite ale Americii privind prelucrarea și transferul datelor din registrul cu numele pasagerilor (PNR), de către transportatorii aerieni, către Departamentul pentru Securitate Internă al Statelor Unite, încheiat în iulie 2007, WP 138.

([4]) Evaluarea de impact, anexa A, „Metode de transmitere a datelor de către transportatori".

100. AEPD ridică un semn de întrebare în privința diferenței între aceste două tipuri de baze de date: faptul că o bază de date pasivă constituie o veritabilă arhivă, cu diferite metode de stocare și extragere a datelor, este pus sub semnul întrebării. Într-adevăr, cele mai multe condiții puse pentru a accesa baza de date pasivă se referă la cerințe de securitate care ar putea fi aplicabile, de asemenea, „bazei de date cu termen de păstrare de cinci ani".

101. Perioada totală de stocare — adică de 13 ani — este, în orice caz, exagerată. Aceasta este motivată în evaluarea de impact prin nevoia de a elabora indicatori de risc și de a stabili modele de călătorie și de comportament ([1]), a căror eficacitate necesită demonstrații suplimentare. De vreme ce este evident că datele pot fi păstrate atât timp cât este necesar într-un caz specific pe toată durata desfășurării anchetei, nicio motivație nu poate sprijini păstrarea datelor tuturor pasagerilor, timp de 13 ani, în absența oricărei suspiciuni.

102. AEPD constată, în continuare, că acest termen de păstrare nu este sprijinit de răspunsurile statelor membre la chestionarul Comisiei, potrivit căruia perioada medie de stocare necesară ar fi de 3 ani și jumătate ([2]).

103. Mai mult, termenul de 13 ani este comparabil cu termenul de păstrare de 15 ani din cel mai recent acord cu Statele Unite. AEPD a înțeles întotdeauna că acest lung termen de păstrare a fost convenit datorită puternicei presiuni a guvernului SUA de a avea un termen mult mai mare de 3 ani și jumătate, și nu datorită faptului că a fost, în vreun moment, cerut de Consiliu sau de Comisie. Nu există niciun motiv de a transpune un astfel de compromis — care a fost justificat ca un rezultat necesar al negocierilor — într-un instrument juridic din cadrul Uniunii Europene.

Rolul Comitetului statelor membre

104. Comitetul statelor membre, constituit prin articolul 14 din propunere, va avea atribuții în privința aspectelor de securitate, inclusiv protocolul și criptarea datelor PNR, dar și în privința îndrumării pentru elaborarea unor criterii, a unor metode și practici generale comune în legătură cu evaluarea de risc.

105. În afara acestor indicații, propunerea nu mai include niciun element sau criteriu cu privire la condițiile concrete și la cadrul procesului de evaluare a riscului. Evaluarea de impact arată că aceste criterii vor depinde, în cele din urmă, de informațiile deținute de fiecare stat membru, și care evoluează în mod constant. Evaluarea de risc trebuie să fie efectuată în absența unor standarde uniforme de identificare a suspecților. Astfel, măsura în care Comitetul statelor membre va putea juca un rol în acest sens ridică, un semn de întrebare.

Securitatea

106. Propunerea detaliază o serie de măsuri de securitate ([3]) care trebuie luate de către UIP, intermediari și alte autorități competente pentru a proteja datele. Luând în considerare importanța bazei de date și sensibilitatea prelucrării, AEPD consideră că, în plus față de măsurile avute în vedere, entitatea care prelucrează datele ar trebui, de asemenea, să fie obligată să informeze în mod oficial cu privire la orice încălcare a normelor de securitate.

107. AEPD are cunoștință de proiectul de a elabora o astfel de procedură de notificare în domeniul comunicațiilor electronice la nivel european. Aceasta propune introducerea unei astfel de garanții în prezenta propunere, și trimite în acest sens la sistemul de alertă în caz de încălcare a normelor de securitate instituit în Statele Unite cu privire la agențiile statale ([4]). Incidentele de securitate pot avea loc, într-adevăr, în orice domeniu de activitate, atât în sectorul privat cât și în cel public, după cum a arătat pierderea recentă a unei întregi baze de date despre cetățeni de către administrația britanică ([5]). Bazele de date de mare capacitate, cum ar fi cea avută în vedere de propunere, ar fi primele, pe o listă a priorităților, care să beneficieze de un astfel de sistem de alertă.

Clauză de reexaminare și de caducitate

108. AEPD constată că trebuie să fie efectuată o reexaminare în termen de trei ani de la intrarea în vigoare a deciziei-cadru, pe baza rapoartelor pregătite de Comisie. Autoritatea recunoaște faptul că această reexaminare, în baza informațiilor furnizate de statele membre, va acorda o atenție deosebită garanțiilor pentru protecția datelor, și va conține punerea în aplicare a metodei „*push*", păstrarea datelor și calitatea evaluării de risc. Pentru a fi cuprinzătoare, o astfel de revizuire ar trebui să conțină rezultatele unei analize a datelor statistice generate pe baza prelucrării informațiilor din PNR. Aceste statistici ar trebui să conțină, în plus față de elementele menționate la articolul 18 din propunere, detalii statistice privind identificarea persoanelor de mare risc, cum ar fi criteriile pentru o astfel de identificare și rezultatele concrete ale oricărei măsuri de aplicare a legii luate ca urmare a identificării.

([1]) Evaluarea de impact, anexa A, „Termenul de păstrare a datelor".
([2]) Evaluarea de impact, anexa B.
([3]) Articolul 12 din propunere.
([4]) A se vedea, în special, lucrările organismului american „Identity Theft Task Force", http://www.idtheft.gov/
([5]) A se vedea adresa site-ului Administrației britanice fiscale și vamale a Majestății Sale: http://www.hmrc.gov.uk/childbenefit/update-faqs.htm
A se vedea, de asemenea: http://news.bbc.co.uk/1/hi/uk_politics/7103566.stm

109. AEPD a insistat, deja, în avizul său, asupra absenței elementelor concrete pentru stabilirea necesității sistemului propus. Autoritatea consideră, cu toate acestea, că decizia-cadru ar trebui, cel puțin, completată printr-o clauză de caducitate în cazul în care aceasta ar intra în vigoare. La finalul termenului de trei ani, decizia-cadru ar trebui să fie abrogată în cazul în care nu ar interveni niciun element în sprijinul continuării aplicării sale.

Impactul asupra altor instrumente juridice

110. În dispozițiile sale finale, propunerea impune o condiție aplicării în continuare a acordurilor sau a înțelegerilor bilaterale sau multilaterale aflate în vigoare. Aceste instrumente pot fi aplicate numai în limita în care sunt compatibile cu obiectivele deciziei-cadru propuse.

111. AEPD consideră că domeniul de aplicare al acestei dispoziții ridică semne de întrebare. După cum s-a menționat deja la capitolul V, subtitlul „Reciprocitate", nu este clar dacă această dispoziție va avea impact asupra conținutului acordului cu țările terțe, cum ar fi acordul cu SUA. Din alt punct de vedere, nu este, de asemenea, clar dacă dispoziția ar putea avea un impact asupra condițiilor de aplicare a instrumentelor cu un domeniul mai larg de aplicare, cum ar fi Convenția nr. 108 a Consiliului Europei. Cu toate că poate părea puțin probabil, având în vedere contextul instituțional diferit și actorii implicați, ar trebui evitat orice risc de interpretare greșită, iar propunerea ar trebui să clarifice faptul că nu influențează instrumentele cu un domeniu mai larg de aplicare, în special cele având drept scop protecția drepturilor fundamentale.

VII. **CONCLUZIE**

112. AEPD insistă asupra impactului major al prezentei propuneri în ce privește protecția datelor. Autoritatea și-a concentrat analiza asupra a patru probleme fundamentale ridicate de propunere, și insistă asupra faptului că acestea trebuie să fie abordate într-o manieră cuprinzătoare. În cadrul circumstanțelor actuale, propunerea nu se conformează drepturilor fundamentale, în special articolul 8 din Carta drepturilor fundamentale a Uniunii Europene, și nu ar trebui adoptată.

113. În cazul în care comentariile anterioare vor fi respectate, în special testul de legitimitate, legiuitorul ar trebui să țină cont de cele câteva propuneri de redactare făcute în prezentul aviz. Se face trimitere, în special, la punctele 67, 73, 77, 80, 90, 93, 106, 109 și 111 din aviz.

Legitimitatea acțiunii propuse

114. Deși scopul general al luptei împotriva terorismului și a criminalității organizate este, în sine, clar și justificat, esența procesului de prelucrare care se va institui nu este suficient circumscrisă și justificată.

115. AEPD consideră că tehnica de a evalua riscul prezentat de persoane prin folosirea instrumentelor de extragere a datelor și a modelelor comportamentale trebuie evaluată în continuare, iar utilitatea acestora trebuie să fie stabilită fără echivoc în cadrul luptei împotriva terorismului, înainte de a fi utilizate pe o scară atât de largă.

116. Exploatarea unor baze de date fără o privire globală asupra rezultatelor concrete și a neajunsurilor:

— este contrară politicilor legislative raționale în care un nou instrument trebuie adoptat numai după punerea completă în aplicare a instrumentelor existente și dovedirea insuficienței acestora.

— poate conduce, în plus, înspre o societate complet supravegheată.

117. Lupta împotriva terorismului poate fi, cu siguranță, un motiv legitim pentru aplicarea excepțiilor la drepturile fundamentale privind viața privată și protecția datelor. Cu toate acestea, pentru a fi valabilă, necesitatea imixtiunii trebuie să fie sprijinită de elemente clare și indubitabile, iar proporționalitatea prelucrării trebuie să fie demonstrată. Aceasta se cere cu atât mai mult în cazul imixtiunii grave în viața privată a indivizilor, după cum se prevede în propunere.

118. Aceste elemente justificative lipsesc în propunere și testele privind necesitatea și proporționalitatea nu sunt îndeplinite.

119. AEPD insistă asupra caracterului esențial al testelor privind necesitatea și proporționalitatea, descrise anterior. Acestea reprezintă o *condicio sine qua non* pentru intrarea în vigoare a propunerii.

Cadrul legal aplicabil

120. AEPD constată o deficiență serioasă de siguranță juridică în privința regimului aplicabil diferiților actori implicați în proiect, în special companiilor aeriene și altor actori din cadrul primului pilon: fie că este vorba de normele din propunere, de normele din decizia-cadru privind protecția datelor sau de legislația națională care transpune Directiva 95/46/CE. Legiuitorul ar trebui să indice cu claritate în ce etapă a prelucrării se aplică fiecare categorie de norme.

121. Tendința actuală de a impune, în mod sistematic, actorilor privați cooperarea în scopul aplicării legii ridică problema cadrului de protecție a datelor (primul sau al treilea pilon) care se aplică condițiilor acestei cooperări: nu este clar dacă normele ar trebui să se întemeieze pe calitatea operatorului de date (sectorul privat) sau pe scopul urmărit (aplicarea legii).

122. AEPD a insistat deja asupra riscului unei lacune în legislație în cazul activităților ce țin de primul și de al treilea pilon ([1]). Nu este, într-adevăr, deloc clar dacă măsurile întreprinderilor private, care au legătură într-un fel sau altul cu aplicarea dreptului penal, intră în sfera de acțiune a legiuitorului Uniunii Europene în conformitate cu articolele 30, 31 și 34 din Tratatul UE.

123. Ar trebui evitat un rezultat în care prelucrarea de către prestatorii de servicii în diferite scopuri ar fi supusă unor cadre diferite pentru protecția datelor, în special luând în considerare dificultățile pe care acesta le-ar crea în ce privește exercitarea drepturilor de către persoanele vizate.

Calitatea destinatarilor

124. Propunerea ar trebui să prevadă o specificare cu privire la calitatea destinatarilor datelor cu caracter personal colectate de companiile aeriene, fie că e vorba de intermediari, unități de informații despre pasageri sau autorități competente.

125. Calitatea destinatarului, care în anumite cazuri ar putea fi actor din sectorul privat, este în raport direct cu tipul de garanții privind protecția datelor aplicabile acelui destinatar. Este esențial ca regimul aplicabil să fie clar pentru toți actorii implicați, inclusiv pentru legiuitor, autoritățile de protecție a datelor, precum și pentru operatorii de date și persoanele vizate implicate.

Transferul datelor către țări terțe

126. AEPD insistă asupra necesității de a se asigura că există un nivel adecvat de protecție în țara de destinație. Autoritatea consideră că semnificația principiului „reciprocității" menționat în propunere, precum și aplicarea acestuia în țări deja angajate în acorduri cu Uniunea Europeană, cum sunt Canada și SUA, ridică, de asemenea, semne de întrebare. Aceasta consideră de maximă importanță coerența condițiilor pentru transferul datelor PNR către țări terțe și conformitatea acestora cu un nivel armonizat de protecție.

Alte aspecte importante

127. AEPD atrage, de asemenea, atenția legiuitorului către aspectele specifice ale propunerii care necesită mai multă precizie sau o mai bună integrare a principiului protecției datelor. Este cazul, în special, în legătură cu următoarele aspecte:

— ar trebui restricționate condițiile în care se pot lua decizii automate,

— cantitatea de date prelucrate ar trebui redusă,

— transferul de date ar trebui să se bazeze exclusiv pe metoda „*push*",

— termenul de păstrare a datelor este considerat ca fiind excesiv și nejustificat,

— rolul comitetului statelor membre ar putea fi mai precis în privința îndrumării acestuia pentru realizarea „evaluării de risc",

— măsurile de securitate ar trebui să includă o procedură de „notificare în caz de încălcare a normelor de securitate",

— reexaminarea deciziei ar trebui să includă o clauză de caducitate,

— propunerea ar trebui să clarifice faptul că nu are nicio influență asupra instrumentelor cu un domeniu de aplicare mai larg având, în special, drept scop protecția drepturilor fundamentale.

Observații finale

128. AEPD constată că prezenta propunere este făcută într-un moment în care contextul instituțional al Uniunii Europene este pe cale să sufere o schimbare fundamentală. Consecințele Tratatului de la Lisabona în ce privește luarea deciziilor vor fi fundamentale, în special în ceea ce privește rolul Parlamentului.

129. Luând în considerare impactul fără precedent al propunerii în privința drepturilor fundamentale, AEPD propune să nu fie adoptată în cadrul stabilit de prezentul tratat, ci să asigure respectarea procedurii de codecizie prevăzute de noul tratat. Astfel se va consolida baza legală în care vor fi luate acțiunile decisive avute în vedere în propunere.

([1]) A se vedea avizul Autorității Europene pentru Protecția Datelor privind comunicarea Comisiei către Parlamentul European și Consiliu cu privire la continuarea programului de lucru pentru o mai bună punere în aplicare a directivei privind protecția datelor (JO C 255, 27.10.2007, p. 1). A se vedea, de asemenea, Raportul anual 2006, p. 47.