Avizul Autorității Europene pentru Protecția Datelor referitor la propunerea de directivă a Parlamentului European și a Consiliului privind utilizarea datelor din registrul cu numele pasagerilor pentru prevenirea, depistarea, cercetarea și urmărirea penală a infracțiunilor de terorism și a infracțiunilor grave

(2011/C 181/02)

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 articolele 7 și 8,

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

având în vedere solicitarea unui aviz formulată în conformitate cu articolul 28 alineatul (2) din 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],

ADOPTĂ PREZENTUL AVIZ:

I. INTRODUCERE

I.1. *Consultarea AEPD*

1. La 2 februarie 2011, Comisia a adoptat o propunere de directivă a Parlamentului European și a Consiliului privind utilizarea datelor din registrul cu numele pasagerilor pentru prevenirea, depistarea, cercetarea și urmărirea penală a infracțiunilor de terorism și a infracțiunilor grave (denumită în continuare „propunerea") [3]. Propunerea a fost transmisă AEPD spre consultare în aceeași zi.

2. AEPD salută faptul că a fost consultată de către Comisie. AEPD a avut ocazia de a formula observații neoficiale chiar înainte de adoptarea propunerii. Unele dintre aceste observații au fost luate în considerare în propunere, iar AEPD ia notă de faptul că au fost în general întărite garanțiile de protecție a datelor cuprinse în propunere. Cu toate acestea, există în continuare motive de îngrijorare privind anumite aspecte, în special în legătură cu amploarea și scopurile colectării datelor cu caracter personal.

I.2. *Propunerea în contextul său*

3. Discuțiile privind un posibil sistem PNR pe teritoriul UE se desfășoară din 2007, când Comisia a adoptat o propunere de decizie-cadru a Consiliului pe această temă [4]. Principalul scop al instituirii unui sistem PNR UE este acela de a obliga transportatorii aerieni care operează zboruri internaționale între UE și țări terțe să transmită către autoritățile competente datele PNR privind toți pasagerii, în scopul prevenirii, depistării, cercetării și urmăririi penale a infracțiunilor de terorism și a infracțiunilor grave. Datele ar urma să fie centralizate și analizate de către unitățile de informații despre pasageri, iar rezultatul analizei ar urma să fie transmis autorităților naționale competente din fiecare stat membru.

4. Din 2007, AEPD a urmărit îndeaproape evoluțiile legate de un posibil sistem PNR UE, în paralel cu evoluțiile privind sistemele PNR din țările terțe. La 20 decembrie 2007, AEPD a adoptat un aviz privind această propunere a Comisiei [5]. În multe alte ocazii, nu doar AEPD, ci și Grupul de lucru pentru protecția persoanelor în ceea ce privește prelucrarea datelor cu caracter personal [6] au formulat în mod consecvent observații cu privire la respectarea principiului necesității și al proporționalității, precum și a altor garanții esențiale de protecție a datelor, în cazul prelucrării datelor PNR în scopul aplicării legii.

5. Principalul aspect ridicat în mod consecvent de către AEPD se referă la justificarea necesității unui sistem PNR european pe lângă numeroasele instrumente existente care permit prelucrarea datelor cu caracter personal în scopul aplicării legii.

6. AEPD confirmă îmbunătățirile vizibile din punctul de vedere al protecției datelor aduse prin prezenta propunere comparativ cu versiunea asupra căreia și-a exprimat avizul anterior. Aceste îmbunătățiri se referă în special la domeniul de aplicare al propunerii, definirea rolului diferitelor părți interesate (unitățile de informații despre pasageri), excluderea prelucrării datelor sensibile, trecerea către un sistem de tip „push" fără o perioadă de tranziție [7] și limitarea perioadei de păstrare a datelor.

---

[1] JO L 281, 23.11.1995, p. 31.
[2] JO L 8, 12.1.2001, p. 1.
[3] COM(2011) 32 final.
[4] COM(2007) 654 final.
[5] Avizul AEPD din 20 decembrie 2007 referitor la propunerea de decizie-cadru a Consiliului privind utilizarea datelor din registrul cu numele pasagerilor (PNR) în scopul aplicării legii, JO C 110, 1.5.2008, p. 1.
[6] — Avizul din 19 octombrie 2010 privind o abordare globală referitoare la transferul de date din registrul cu numele pasagerilor (PNR) către țări terțe, disponibil la: http://www.AEPD.europa.eu/AEPDWEB/AEPD/Consultation/OpinionsC/OC2010
— Avizele Grupului de lucru pentru protecția persoanelor în ceea ce privește prelucrarea datelor cu caracter personal sunt disponibile la următorul link: http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/index_en.htm#data_transfers
[7] Acest lucru înseamnă că datele PNR vor fi transmise în mod activ de către transportatorii aerieni și nu vor mai fi extrase de către autoritățile publice prin accesarea directă a bazei de date a transportatorilor aerieni.

7. AEPD salută, de asemenea, evoluțiile suplimentare din analiza de impact privind motivele introducerii unui sistem PNR UE. Cu toate acestea, deși există o dorință vizibilă de a clarifica necesitatea sistemului, AEPD nu găsește în cadrul acestor noi justificări o bază convingătoare pentru crearea sistemului, în special în ceea ce privește „evaluarea prealabilă" pe scară largă a tuturor pasagerilor. Necesitatea și proporționalitatea sunt analizate mai jos, la capitolul II. Capitolul III se concentrează asupra unor aspecte specifice ale propunerii.

II. **NECESITATEA ȘI PROPORȚIONALITATEA PROPUNERII**

II.1. *Observații preliminare privind necesitatea și proporționalitatea*

8. Demonstrarea necesității și proporționalității prelucrării datelor reprezintă o premisă esențială pentru crearea sistemului PNR. AEPD a insistat deja cu alte ocazii, în special în contextul posibilei revizuiri a Directivei 2006/24/CE („Directiva privind păstrarea datelor"), asupra faptului că nevoia de prelucrare sau stocare a unor cantități enorme de informații ar trebui să se bazeze pe o demonstrare clară a relației dintre *utilizare* și *rezultat* și să permită o evaluare *sine qua non* a posibilității de a obține rezultate comparabile prin mijloace alternative, mai puțin invazive asupra vieții private ([1]).

9. În vederea justificării sistemului, propunerea și în special analiza de impact care o însoțește includ o documentație amplă și argumente juridice pentru a stabili atât necesitatea sistemului, cât și conformitatea acestuia cu cerințele privind protecția datelor. Se merge chiar mai departe, susținându-se chiar că sistemul aduce valoare adăugată din punctul de vedere al armonizării standardelor de protecție a datelor.

10. După analizarea acestor elemente, AEPD consideră că propunerea, în forma sa actuală, *nu* respectă cerințele de necesitate și proporționalitate impuse de articolul 8 din Carta drepturilor fundamentale a Uniunii Europene, articolul 8 din Convenția europeană a drepturilor omului și articolul 16 din Tratatul privind funcționarea Uniunii Europene. Raționamentul care stă la baza acestei considerații este prezentat în alineatele următoare.

II.2. *Documente și statistici puse la dispoziție de către Comisie*

11. AEPD ia notă de faptul că analiza de impact cuprinde explicații și statistici detaliate în vederea justificării propunerii. Totuși, aceste elemente nu sunt convingătoare. De exemplu, descrierea amenințării pe care o reprezintă terorismul și infracționalitatea gravă, inclusă în analiza de impact și în expunerea de motive a propunerii ([2]), indică un număr de 14 000 de infracțiuni la 100 000 de locuitori în statele membre, în 2007. Deși acest număr este impresionant, se referă la tipuri nediferențiate de infracțiuni și nu poate fi invocat pentru justificarea unei propuneri care vizează și combate doar un număr limitat de infracțiuni grave transnaționale și acte de terorism. Un alt exemplu constă în faptul că citarea unui raport privind „problemele" reprezentate de droguri, fără corelarea statisticilor cu tipul de trafic de droguri avut în vedere în propunere, nu reprezintă, în opinia AEPD, o referință valabilă. Același lucru este valabil și în ceea ce privește indicarea consecințelor infracțiunilor, respectiv „valoarea bunurilor furate" și impactul psihologic și fizic asupra victimelor, aceste date neavând o legătură directă cu scopul propunerii.

12. Ca ultim exemplu, în analiza de impact se specifică faptul că Belgia a „raportat că 95 % din totalul capturilor de droguri efectuate în 2009 s-a datorat, în mod exclusiv sau predominant, prelucrării datelor PNR". Cu toate acestea, trebuie subliniat faptul că Belgia nu a pus (încă) în aplicare un sistem PNR organizat, comparabil cu cel prevăzut în propunere. Acest lucru ar putea însemna că datele PNR pot fi utile în cazuri specifice, ceea ce AEPD nu contestă, însă colectarea vastă în vederea unei evaluări sistematice a tuturor pasagerilor ridică probleme serioase din punctul de vedere al protecției datelor.

13. AEPD consideră că nu există o documentație generală relevantă, corectă și suficientă care să justifice necesitatea instrumentului.

II.3. *Condiții pentru limitarea unui drept fundamental*

14. Deși documentul menționează faptul că măsurile de prelucrare a datelor interferează cu Carta, cu Convenția europeană a drepturilor omului și cu articolul 16 din Tratatul privind funcționarea Uniunii Europene, acesta se referă în mod direct la posibilele limitări ale acestor drepturi și se mulțumește cu concluzia că „întrucât acțiunile propuse vizează combaterea terorismului și a altor infracțiuni grave, atunci când acestea ar fi incluse într-un act legislativ ar respecta în mod cert aceste cerințe, cu condiția să fie necesare într-o societate democratică și să respecte principiul proporționalității" ([3]). Cu toate acestea, nu se demonstrează în mod clar că măsurile sunt esențiale și că nu există alte alternative mai puțin invazive.

15. În acest sens, faptul că unele obiective suplimentare precum aplicarea măsurilor împotriva imigrației ilegale, „lista persoanelor care au interdicție de zbor" și siguranța din punctul de vedere al stării de sănătate au fost avute în vedere și, în cele din urmă, nu au fost incluse din considerente legate de proporționalitate nu înseamnă că „limitarea" prelucrării datelor PNR la cazurile de infracțiuni grave și terorism este *de facto* proporțională întrucât este mai puțin invazivă. Nici opțiunea de a limita sistemul la combaterea terorismului, fără a include infracțiuni suplimentare, astfel cum s-a avut în vedere în sistemele PNR anterioare, în special în fostul sistem PNR australian, nu a fost supusă unei evaluări. AEPD subliniază faptul că în cadrul acestui sistem anterior, în privința căruia Grupul de lucru pentru protecția persoanelor în ceea ce

([1]) A se vedea discursul lui Peter Hustinx „Momentul adevărului pentru Directiva privind păstrarea datelor", expus în cadrul conferinței „Taking on the Data Retention Directive" („Să discutăm despre Directiva privind păstrarea datelor"), Bruxelles, 3 decembrie 2010, disponibil la: http://www.AEPD.europa.eu/AEPDWEB/webdav/site/mySite/shared/Documents/AEPD/Publications/Speeches/2010/10-12-03_Data_retention_speech_PH_EN.pdf

([2]) Analiza de impact, capitolul 2.1.1 și expunerea de motive, capitolul 1, alineatul (1).

([3]) Analiza de impact, capitolul 3.2, al alineatul (2).

privește prelucrarea datelor cu caracter personal a adoptat un aviz pozitiv în 2004, obiectivele se limitau la „identificarea pasagerilor care ar putea reprezenta o amenințare din punctul de vedere al terorismului sau al activităților infracționale asociate” ([1]). De asemenea, sistemul australian nu prevedea păstrarea datelor PNR decât în cazul pasagerilor specifici identificați ca reprezentând o amenințare specifică ([2]).

16. În plus, în ceea ce privește caracterul previzibil al supravegherii subiecților datelor, nu este tocmai cert că propunerea Comisiei îndeplinește cerințele unui temei juridic solid conform legislației comunitare: „evaluarea” pasagerilor (denumită anterior „evaluarea riscurilor”) va fi efectuată pe baza unor criterii netransparente și aflate în continuă schimbare. După cum s-a afirmat în mod explicit în text, principalul scop al sistemului nu este utilizarea în cadrul controlului tradițional la frontieră, ci ca instrument de informații ([3]) și arestare a unor persoane care nu sunt suspecte, înainte de săvârșirea unei infracțiuni. Elaborarea la scară europeană a unui astfel de sistem, care să implice colectarea datelor tuturor pasagerilor și luarea de decizii pe baza unor criterii de evaluare necunoscute și în continuă schimbare, ridică grave probleme de transparență și proporționalitate.

17. Singurul scop care, în opinia AEPD, ar respecta cerințele privind transparența și proporționalitatea ar fi utilizarea datelor PNR de la caz la caz, după cum se menționează la articolul 4.2 litera (c), însă doar în situația unei amenințări grave și concrete stabilite pe baza unor indicatori concreți.

II.4. *Riscul de denaturare a funcțiilor*

18. Articolul 4 alineatul (2) litera (b) prevede că o unitate de informații despre pasageri poate să efectueze o evaluare a pasagerilor, iar în cadrul acestei activități poate să confrunte datele PNR cu „bazele de date relevante”, după cum se indică la articolul 4.2 litera (b). Această dispoziție nu precizează care sunt bazele de date relevante. Prin urmare, măsura nu este previzibilă, cerință impusă prin Cartă și Convenția europeană a drepturilor omului. În plus, dispoziția ridică problema compatibilității sale cu principiul limitării scopului: în opinia AEPD, aceasta ar trebui exclusă, de exemplu, în cazul unei baze de date precum Eurodac care a fost creată pentru a servi unor scopuri diferite ([4]). În plus, acest lucru ar trebui să fie posibil doar atunci când există o nevoie specifică, în cazul particular al unei suspiciuni prealabile cu privire la o anumită persoană, după săvârșirea unei infracțiuni. De exemplu, confruntarea sistematică a bazei de date a Sistemului de informații privind vizele ([5]) cu toate datele PNR ar fi excesivă și disproporționată.

II.5. *Valoarea adăugată a propunerii din punctul de vedere al protecției datelor*

19. Ideea conform căreia propunerea ar spori protecția datelor prin faptul că asigură un cadru omogen și uniform în ceea ce privește drepturile persoanelor este discutabilă. AEPD confirmă faptul că, în cazul în care necesitatea și proporționalitatea sistemului ar fi stabilite, standardele uniforme la nivelul UE, inclusiv în domeniul protecției datelor, ar consolida securitatea juridică. Cu toate acestea, în formularea sa actuală, propunerea menționează la considerentul 28 că „directiva nu aduce atingere posibilității statelor membre de a prevedea, în temeiul legislației lor naționale, un sistem de colectare și de gestionare a datelor PNR în alte scopuri decât cele prevăzute în prezenta directivă sau de a colecta și gestiona date provenind de la alți transportatori decât cei menționați în directivă, referitoare la zborurile interne (…)”.

20. Armonizarea introdusă de propunere este, așadar, limitată. Este adevărat că se referă la drepturile subiecților datelor, însă nu și la limitarea scopului, și se poate presupune că, în conformitate cu această formulare, sistemele PNR folosite deja pentru combaterea imigrației ilegale ar putea fi folosite în continuare în același scop și în temeiul directivei.

21. Acest lucru înseamnă că, pe de o parte, ar exista în continuare anumite diferențe între statele membre care au elaborat deja un sistem PNR, iar pe de altă parte marea majoritate a statelor membre care nu colectează în mod sistematic date PNR (21 din 27 de state membre) ar fi obligate să procedeze astfel. AEPD consideră că, din această perspectivă, orice valoare adăugată din punctul de vedere al protecției datelor este extrem de discutabilă.

([1]) Avizul 1/2004 din 16 ianuarie 2004 privind nivelul de protecție asigurat în Australia pentru transmiterea datelor din registrul cu numele pasagerilor de către transportatorii aerieni, Grupul de lucru 85.

([2]) În avizul Grupului de lucru pentru protecția persoanelor în ceea ce privește prelucrarea datelor cu caracter personal se explică, în plus, că „în ceea ce privește păstrarea datelor PNR, vămilor nu le este impusă prin lege nicio obligație de a păstra datele PNR. De asemenea, nu le este impusă nicio interdicție privind stocarea acestor date. Datele PNR ale pasagerilor evaluați prin programe informatice automatizate de analiză a profilului și considerate, în urma evaluării, ca fiind de risc scăzut (în cazul a 95 %-97 % dintre pasageri) nu sunt păstrate și nu se ține nicio evidență a informațiilor PNR ale acestora. Așadar, vămile aplică o politică generală de nepăstrare a acestor date. Pentru cei 0,05 %-0,1 % dintre pasageri care sunt trimiși autorităților vamale în vederea unei evaluări mai amănunțite, datele PNR transmise de către transportatorul aerian sunt păstrate temporar până la finalizarea evaluării vamale, însă nu sunt stocate. După finalizarea evaluării, datele PNR ale pasagerilor respectivi sunt șterse din calculatorul ofițerului unității de analiză a pasagerilor (PAU) din cadrul autorității vamale și nu sunt introduse în bazele de date australiene.”.

([3]) Expunere de motive, capitolul 1. Contextul propunerii, Coerența cu celelalte politici și obiective ale UE.

([4]) Obiectivul Eurodac „este să contribuie la determinarea statului membru responsabil, în temeiul Convenției de la Dublin, cu examinarea unei cereri de azil prezentate într-un stat membru și, pe de altă parte, să faciliteze aplicarea Convenției de la Dublin în condițiile stabilite de prezentul regulament”, în conformitate cu articolul 1 alineatul (1) din Regulamentul (CE) nr. 2725/2000 al Consiliului din 11 decembrie 2000 privind instituirea sistemului „Eurodac” pentru compararea amprentelor digitale în scopul aplicării eficiente a Convenției de la Dublin, JO L 316, 15.12.2000, p. 1.

([5]) „VIS urmărește îmbunătățirea punerii în aplicare a politicii comune în materie de vize, a cooperării la nivel consular și a consultărilor care au loc între autoritățile centrale responsabile în domeniul vizelor prin facilitarea schimbului de date între statele membre cu privire la cererile de viză și la deciziile referitoare la acestea”, în conformitate cu articolul 2 din Regulamentul (CE) nr. 767/2008 al Parlamentului European și al Consiliului din 9 iulie 2008 privind Sistemul de informații privind vizele (VIS) și schimbul de date între statele membre cu privire la vizele de scurtă ședere (Regulamentul VIS), JO L 218, 13.8.2008, p. 60.

22. Dimpotrivă, consecințele considerentului 28 constau într-o încălcare gravă a principiului limitării scopului. În opinia AEPD, propunerea ar trebui să prevadă în mod explicit faptul că folosirea datelor PNR în alte scopuri este interzisă.

23. AEPD a ajuns la o concluzie similară cu cea formulată în urma evaluării Directivei privind păstrarea datelor: în ambele contexte, lipsa unei armonizări reale este însoțită de o lipsă a securității juridice. În plus, colectarea și prelucrarea suplimentară a datelor cu caracter personal devine obligatorie pentru toate statele membre, deși necesitatea reală a sistemului nu a fost încă stabilită.

II.6. *Corelarea cu Comunicarea privind modul de gestionare a informațiilor în spațiul de libertate, securitate și justiție*

24. În plus, AEPD ia notă de faptul că evoluțiile privind PNR sunt corelate cu evaluarea generală permanentă a tuturor instrumentelor UE în domeniul gestionării schimburilor de informații lansate de către Comisie în ianuarie 2010 și dezvoltate în comunicarea recentă privind prezentarea generală asupra modului de gestionare a informațiilor în spațiul de libertate, securitate și justiție ([1]). Există, în special, o legătură clară cu dezbaterea actuală privind strategia europeană de gestionare a informațiilor. În această privință, AEPD consideră că în cadrul evaluării necesității unui sistem UE PNR ar trebui avute în vedere mai ales rezultatele activității actuale privind modelul european de schimb de informații preconizat pentru 2012.

25. În acest context și ținând seama de deficiențele propunerii, în special de cele ale analizei de impact care o însoțește, AEPD consideră că este necesară o analiză de impact specifică în ceea ce privește confidențialitatea și protecția datelor în cazuri precum acesta, în care fondul propunerii afectează drepturile fundamentale la viață privată și protecția datelor. Nu este suficientă o analiză generală de impact.

III. **OBSERVAȚII SPECIFICE**

III.1. *Domeniul de aplicare*

26. Infracțiunile de terorism, infracțiunile grave și infracțiunile grave transfrontaliere sunt definite la articolul 2 literele (g), (h) și (i) din propunere. AEPD salută faptul că definițiile – și domeniul de aplicare a acestora – au fost îmbunătățite, introducându-se diferențierea între infracțiunile grave și infracțiunile grave transnaționale. Această distincție este binevenită în special datorită faptului că implică o prelucrare diferită a datelor cu caracter personal, excluzând evaluarea în baza unor criterii predeterminate atunci când este vorba despre infracțiuni grave care nu sunt transnaționale.

27. Cu toate acestea, definiția infracțiunilor grave este în continuare prea generală, în opinia AEPD. Acest lucru este confirmat în propunere, unde se indică faptul că statele membre pot, totuși, să excludă *infracțiunile de mică gravitate* care se înscriu în definiția infracțiunilor grave ([2]), însă care nu ar fi conforme cu principiul proporționalității. Această formulare implică faptul că definiția cuprinsă în propunere ar putea foarte ușor să includă infracțiuni de mică gravitate, a căror prelucrare ar fi disproporționată. Nu este foarte clar care infracțiuni se pot înscrie în categoria celor minore. AEPD consideră că, în loc să lase restrângerea domeniului de aplicare la latitudinea statelor membre, propunerea ar trebui să enumere în mod explicit infracțiunile care ar trebui incluse în domeniul său de aplicare, precum și pe cele care ar trebui excluse, pe considerentul că sunt minore și nu îndeplinesc criteriul proporționalității.

28. Același motiv de preocupare este valabil și în ceea ce privește posibilitatea neclarificată la articolul 5 alineatul (5), referitoare la prelucrarea datelor privind orice tip de infracțiuni în cazul în care sunt depistate în cursul aplicării legii, precum și posibilitatea menționată la considerentul 28 în legătură cu extinderea domeniului de aplicare către scopuri diferite de cele prevăzute în propunere sau către alți transportatori.

29. De asemenea, AEPD este preocupată de posibilitatea, prevăzută la articolul 17, de a include zborurile interne în domeniul de aplicare a directivei, având în vedere experiența dobândită de către statele membre care colectează deja acest tip de date. O astfel de extindere a domeniului de aplicare a sistemului PNR ar amenința și mai mult drepturile fundamentale ale persoanelor și nu ar trebui avută în vedere înainte de efectuarea unei analize corespunzătoare, inclusiv a unei analize de impact cuprinzătoare.

30. În concluzie, faptul că domeniul de aplicare a rămas deschis și faptul că se acordă statelor membre posibilități de extindere a scopului încalcă cerința conform căreia datele trebuie să fie colectate doar în scopuri specificate și explicite.

III.2. *Unitățile de informații despre pasageri*

31. Rolul unităților de informații despre pasageri și garanțiile legate de prelucrarea datelor PNR ridică întrebări specifice, în special ținând seama de faptul că unitățile de informații despre pasageri primesc de la transportatori date privind toți pasagerii și au – conform textului propunerii – competențe vaste de prelucrare a acestor date. Acestea includ evaluarea comportamentului pasagerilor care nu sunt suspectați de nicio infracțiune și posibilitatea de a corela datele PNR cu baze de date neprecizate ([3]). AEPD ia notă de faptul că propunerea prevede condiții de „acces limitat”, însă consideră că doar aceste condiții nu sunt suficiente având în vedere competențele vaste ale unităților de informații despre pasageri.

32. În primul rând, natura autorității desemnate drept unitate de informații despre pasageri și structura acesteia nu sunt clarificate. Propunerea menționează posibilitatea ca membrii personalului să poată fi „detașați de la autoritățile publice competente”, însă nu oferă nicio garanție din punctul de vedere al competenței și integrității personalului unităților

([1]) COM(2010) 385 final.

([2]) După cum se menționează în Deciziile-cadru 2008/841/JAI și 2002/584/JAI ale Consiliului.

([3]) În legătură cu unitățile de informații despre pasageri, a se vedea de asemenea Avizul AEPD din 20 decembrie 2007.

de informații despre pasageri. AEPD recomandă includerea acestor cerințe în textul directivei, ținând seama de caracterul sensibil al prelucrării ce trebuie efectuată de către unitățile de informații despre pasageri.

33. În al doilea rând, propunerea permite desemnarea unei singure unități de informații despre pasageri pentru mai multe state membre. Acest lucru generează riscuri de utilizare eronată și transmitere a datelor fără respectarea condițiilor incluse în propunere. AEPD recunoaște că unirea forțelor ar putea fi justificată prin motive legate de eficiență, în special în cazul statelor membre mai mici, însă recomandă includerea în text a unor condiții pentru această opțiune. Aceste condiții ar trebui să se refere la cooperarea cu autoritățile competente, precum și la control, în special cu privire la autoritatea de protecție a datelor responsabilă cu supravegherea și la exercitarea drepturilor persoanei vizate, întrucât este posibil ca mai multe autorități să aibă competența de a supraveghea o singură unitate de informații despre pasageri.

34. În legătură cu elementele menționate mai sus există riscul de denaturare a funcțiilor, ținând seama în special de calitatea personalului care are competența să analizeze datele și de „partajarea" unei unități de informații despre pasageri între mai multe state membre.

35. În al treilea rând, AEPD pune sub semnul întrebării garanțiile prevăzute împotriva abuzului. Obligațiile privind ținerea evidenței sunt binevenite, însă nu și suficiente. Automonitorizarea ar trebui completată cu monitorizarea externă, într-o manieră mai structurată. AEPD propune organizarea de audituri în mod sistematic, la interval de patru ani. Ar trebui elaborat un set cuprinzător de norme de securitate care să fie impus pe orizontală tuturor unităților de informații despre pasageri.

III.3. *Schimbul de date între statele membre*

36. Articolul 7 din propunere prevede mai multe scenarii care permit schimbul de date între unitățile de informații despre pasageri – aceasta fiind situația normală – sau între autoritățile competente ale unui stat membru și unitățile de informații despre pasageri, în situații excepționale. De asemenea, condițiile sunt mai stricte în funcție de măsura în care este solicitat accesul la baza de date prevăzută la articolul 9 alineatul (1), în care datele sunt păstrate în primele 30 de zile, sau la baza de date menționată la articolul 9 alineatul (1), în care datele sunt păstrate pentru o perioadă suplimentară de cinci ani.

37. Condițiile de acces sunt definite mai strict atunci când cererea de acces nu urmează procedura normală. Cu toate acestea, AEPD ia notă de faptul că formularea folosită generează confuzii: articolul 7 alineatul (2) este aplicabil într-un „caz specific de prevenire, depistare, cercetare și urmărire penală a infracțiunilor teroriste sau a infracțiunilor grave"; articolul 7 alineatul (3) menționează „situații excepționale, ca răspuns la o amenințare specifică sau în cadrul unei cercetări sau urmăriri penale specifice având ca obiect infracțiuni de terorism sau infracțiuni grave", în timp ce articolul 7 alineatul (4) se referă la „amenințarea gravă și imediată la adresa securității publice", iar articolul 7 alineatul (5) menționează „amenințarea specifică și reală având legătură cu infracțiuni teroriste sau cu infracțiuni grave". Condițiile privind accesarea bazelor de date de către diferitele părți interesate variază în funcție de aceste criterii. Cu toate acestea, diferența dintre o amenințare specifică, o amenințare gravă și imediată și o amenințare specifică și reală nu este clară. AEPD subliniază nevoia unei specificări mai clare a condițiilor exacte în care vor fi permise transferurile de date.

III.4. *Legea aplicabilă*

38. Propunerea face trimitere la Decizia-cadru 2008/977/JAI a Consiliului, ca temei juridic general pentru principiile privind protecția datelor și își lărgește domeniul de aplicare adăugând prelucrarea datelor la nivel intern.

39. AEPD a subliniat deja în 2007 [1] deficiențele deciziei-cadru în ceea ce privește drepturile subiecților datelor. Printre elementele care lipsesc din decizia-cadru se numără în special anumite cerințe în ceea ce privește informațiile puse la dispoziția persoanei vizate în cazul în care aceasta solicită acces la datele sale: informațiile ar trebui formulate într-o formă inteligibilă, ar trebui indicat scopul prelucrării și este necesară introducerea unor garanții mai puternice în cazul în care se apelează la autoritatea de protecție a datelor atunci când accesul direct este refuzat.

40. Trimiterea la decizia-cadru are consecințe și în ceea ce privește identificarea autorității de protecție a datelor care are competența de a monitoriza aplicarea viitoarei directive, întrucât nu este neapărat necesar ca aceasta să fie aceeași cu autoritatea de protecție a datelor care a fost competentă în chestiunile legate de (fostul) prim pilon. AEPD consideră nesatisfăcătoare folosirea deciziei-cadru ca unic temei juridic în contextul post-Lisabona, în condițiile în care unul dintre principalele obiective constă în adaptarea cadrului legal pentru a asigura un nivel ridicat și armonizat de protecție la nivelul (foștilor) piloni. Autoritatea consideră că în propunere ar trebui introduse dispoziții suplimentare care să completeze trimiterea la decizia-cadru a Consiliului acolo unde au fost identificate deficiențe, în special în legătură cu condițiile de accesare a datelor cu caracter personal.

41. Aceste preocupări sunt valabile în egală măsură și în ceea ce privește dispozițiile privind transferurile de date către țări terțe. Propunerea face trimitere la articolul 13 alineatul (3) litera (ii) din decizia-cadru, care include excepții extinse de la garanțiile privind protecția datelor: aceasta oferă în special o derogare de la cerința privind caracterul adecvat în cazul „intereselor legitime prioritare, în special al intereselor publice importante". Această excepție are o formulare vagă, care teoretic s-ar putea aplica în multe cazuri de prelucrare a datelor PNR, dacă este interpretată în sens larg. AEPD consideră că propunerea ar trebui să împiedice în mod explicit aplicarea excepțiilor deciziei-cadru în contextul prelucrării datelor PNR și să mențină cerința unei evaluări stricte a caracterului adecvat.

[1] Al treilea aviz al Autorității Europene pentru Protecția Datelor din 27 aprilie 2007 privind propunerea de decizie-cadru a Consiliului privind protecția datelor cu caracter personal prelucrate în cadrul cooperării polițienești și judiciare în materie penală, JO C 139, 23.6.2007, p. 1.

III.5. *Păstrarea datelor*

42. Propunerea prevede o perioadă de păstrare a datelor de 30 de zile, la care se adaugă o perioadă suplimentară de cinci ani pentru păstrarea datelor în arhivă. Această perioadă de păstrare este redusă substanțial comparativ cu versiunile anterioare ale documentului, în care datele erau păstrate timp de până la cinci ani, la care se adăuga perioada suplimentară de opt ani.

43. AEPD salută reducerea primei perioade de păstrare la 30 de zile. Cu toate acestea, punem sub semnul întrebării perioada de păstrare suplimentară de 5 ani: ni se pare neclar dacă este necesară păstrarea acestor date într-o formă care face în continuare posibilă identificarea persoanelor.

44. De asemenea, AEPD subliniază un aspect legat de terminologia folosită în text, cu consecințe juridice importante: la articolul 9 alineatul (2) se precizează că datele despre pasageri vor fi „acoperite" și prin urmare „li se va da un caracter anonim". Cu toate acestea, textul menționează ulterior că accesul la „integralitatea datelor PNR" este în continuare posibil. Dacă accesul este posibil, înseamnă că datelor PNR nu li s-a dat niciodată un caracter întru totul anonim: deși au caracter anonim, ele rămân în continuare identificabile. Prin urmare, cadrul de protecție a datelor este în continuare pe deplin aplicabil, ceea ce ridică problema fundamentală a necesității și proporționalității păstrării datelor identificabile ale tuturor pasagerilor pe o perioadă de cinci ani.

45. AEPD recomandă ca propunerea să fie reformulată, cu menținerea principiului anonimității reale, fără nicio posibilitate de identificare recursivă a datelor, adică fără a se permite o investigație retroactivă. Aceste date ar putea fi folosite în continuare – și exclusiv – pentru a servi scopurilor generale de colectare a datelor operative pe baza identificării tiparelor actelor de terorism și infracțiunilor asociate în cadrul fluxurilor de migrație. Trebuie făcută distincția între această utilizare și păstrarea datelor în formă identificabilă – sub rezerva anumitor garanții – în cazurile care au generat suspiciuni concrete.

III.6. *Lista datelor PNR*

46. AEPD salută faptul că datele cu caracter sensibil nu sunt incluse în lista datelor care urmează a fi prelucrate. Cu toate acestea, subliniem faptul că propunerea prevede în continuare posibilitatea transmiterii acestor date către unitatea de informații despre pasageri, care are ulterior obligația de a le șterge [articolul 4 alineatul (1), articolul 11]. Din această formulare nu este clar dacă unitățile de informații despre pasageri au obligația permanentă de a filtra datele sensibile transmise de către transportatorii aerieni sau dacă ar trebui să facă acest lucru doar în cazul excepțional în care liniile aeriene le-au trimis din greșeală. AEPD recomandă modificarea textului astfel încât să reiasă în mod clar că nicio dată cu caracter sensibil nu trebuie transmisă de către transportatorii aerieni, care reprezintă sursa prelucrării datelor.

47. Pe lângă datele sensibile, lista datelor care pot fi transferate reflectă în mare măsură lista PNR din SUA, care a fost criticată ca fiind prea amplă în mai multe avize ale Grupului de lucru pentru protecția persoanelor în ceea ce privește prelucrarea datelor cu caracter personal ([1]). AEPD consideră că această listă ar trebui redusă în conformitate cu avizul Grupului de lucru și că orice adăugire trebuie justificată în mod corespunzător. Acest lucru este valabil în special pentru rubrica „mențiuni cu caracter general", care ar trebui exclusă din listă.

III.7. *Deciziile individuale automatizate*

48. În conformitate cu articolul 4.2. literele (a) și (b), evaluarea persoanelor în funcție de criterii predefinite sau prin confruntarea cu bazele de date relevante poate implica prelucrarea automată, însă ar trebui reexaminată individual prin mijloace neautomatizate.

49. AEPD salută clarificările aduse în cadrul acestei noi versiuni a textului. Ambiguitatea versiunii anterioare a domeniului de aplicare a dispoziției în legătură cu deciziile luate pe baza tratamentului automatizat al datelor, care produc „efecte juridice *prejudiciabile* unei persoane sau care *afectează semnificativ* o persoană (…)" a fost înlocuită cu o formulare mai explicită. Acum este clar că orice rezultat pozitiv al unei comparări va fi analizat individual.

50. De asemenea, din versiunea nouă reiese în mod clar că o astfel de evaluare nu poate avea la bază, indiferent de circumstanțe, rasa sau originea etnică a unei persoane, convingerile sale religioase sau filozofice, opiniile politice, apartenența la un sindicat, starea de sănătate sau viața sexuală. Cu alte cuvinte, AEPD înțelege din această nouă formulare că nu se poate lua nicio decizie, nici măcar parțial, pe baza datelor sensibile. Aceasta este în concordanță cu dispoziția conform căreia nici un fel de date sensibile nu pot fi prelucrate de către unitățile de informații despre pasageri, iar acest aspect ar trebui, de asemenea, salutat.

III.8. *Reexaminare și date statistice*

51. AEPD consideră ca fiind extrem de important faptul că se efectuează o evaluare amănunțită a aplicării directivei, după cum se prevede la articolul 17. Considerăm că reexaminarea nu ar trebui doar să evalueze conformitatea generală cu standardele de protecție a datelor, ci și să stabilească, în esență și în detaliu, dacă sistemele PNR reprezintă o măsură necesară. Datele statistice menționate la articolul 18 joacă un rol important din această perspectivă. AEPD consideră că aceste informații ar trebui să includă numărul de acțiuni de aplicare a legii, după cum se prevede în proiectul de text, dar și numărul efectiv de condamnări care au rezultat – sau nu – din acțiunile de aplicare a legii. Aceste date sunt esențiale pentru ca rezultatul reexaminării să fie concludent.

III.9. *Relația cu alte instrumente*

52. Propunerea nu aduce atingere acordurilor existente cu țările terțe (articolul 19). AEPD consideră că această dispoziție ar trebui să se refere mai explicit la obiectivul unui cadru

([1]) Avizul din 23 iunie 2003 privind nivelul de protecție asigurat în Statele Unite pentru transferul datelor pasagerilor, Grupul de lucru 78. Prezentul aviz și avizele ulterioare ale Grupului de lucru în legătură cu acest subiect sunt disponibile la: http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/index_en.htm#data_transfers

global care să prevadă garanții armonizate de protecție a datelor în domeniul PNR, în interiorul și în afara UE, conform cerințelor exprimate de Parlamentul European și detaliate de Comisie în comunicarea din 21 septembrie 2010 „privind o abordare globală referitoare la transferurile de date din registrul cu numele pasagerilor (PNR) către țări terțe".

53. În acest sens, acordurile cu țările terțe nu ar trebui să includă dispoziții aflate sub pragul de protecție a datelor inclus în directivă. Acest lucru este extrem de important în prezent, când se renegociază acordurile cu Statele Unite, Australia și Canada în perspectiva unui cadru global și armonizat.

IV. **CONCLUZIE**

54. Elaborarea unui sistem PNR UE, împreună cu negocierea acordurilor PNR cu țările terțe reprezintă un proiect care se tergiversează de mult timp. AEPD confirmă faptul că proiectul de text a fost supus unor îmbunătățiri vizibile comparativ cu propunerea de decizie-cadru a Consiliului privind PNR UE din 2007. Au fost adăugate garanții de protecție a datelor care au făcut obiectul unor dezbateri și avize ale diferitelor părți interesate, printre care, în special, Grupul de lucru pentru protecția persoanelor în ceea ce privește prelucrarea datelor cu caracter personal, AEPD și Parlamentul European.

55. AEPD salută aceste îmbunătățiri, în special eforturile de limitare a domeniului de aplicare a propunerii și condițiile de prelucrare a datelor PNR. Cu toate acestea, se impune observația că premisa esențială pentru orice dezvoltare a unui sistem PNR – respectiv respectarea principiilor necesității și proporționalității – nu este întrunită în cadrul propunerii. AEPD reamintește că, în opinia sa, datele PNR ar putea fi cu siguranță necesare în scopul aplicării legii în cazuri *specifice* și ele ar putea să respecte cerințele de protecție a datelor. Motivele de îngrijorare specifice se referă la utilizarea acestora într-un mod sistematic și nediferențiat, în legătură cu toți pasagerii.

56. Analiza de impact oferă elemente menite să justifice necesitatea datelor PNR în scopul combaterii infracționalității, însă aceste informații sunt de natură prea generală și nu fundamentează prelucrarea pe scară largă a datelor PNR în scopul colectării de date operative. În opinia AEPD, singura măsură care respectă cerințele de protecție a datelor este utilizarea datelor PNR de la caz la caz, atunci când există o amenințare gravă stabilită pe baza unor indicatori concreți.

57. Pe lângă această deficiență esențială, observațiile AEPD se referă la următoarele aspecte:

— domeniul de aplicare ar trebui să fie mult mai limitat în ceea ce privește tipul infracțiunilor avute în vedere. AEPD pune sub semnul întrebării includerea în propunere a infracțiunilor grave care nu au nicio legătură cu terorismul. În orice caz, infracțiunile minore ar trebui definite în mod explicit și eliminate. AEPD recomandă excluderea posibilității ca statele membre să extindă domeniul de aplicare;

— natura diferitelor amenințări care permit schimbul de date între unitățile de informații despre pasageri sau cu statele membre nu a fost definită într-o măsură suficientă;

— principiile aplicabile privind protecția datelor nu ar trebui să se bazeze doar pe Decizia-cadru 2008/977/JAI a Consiliului, care include anumite deficiențe în special din punctul de vedere al drepturilor subiecților datelor și al transferurilor către țări terțe. În cadrul propunerii ar trebui să se introducă un standard mai ridicat de garanții, bazat pe principiile Directivei 95/46/CE;

— datele nu ar trebui păstrate peste 30 de zile în formă identificabilă, cu excepția cazurilor care justifică derularea unor investigații suplimentare;

— lista datelor PNR care urmează să fie prelucrate ar trebui redusă în conformitate cu recomandările anterioare ale Grupului de lucru pentru protecția persoanelor în ceea ce privește prelucrarea datelor cu caracter personal și ale AEPD. În special rubrica „mențiuni cu caracter general" nu ar trebui să fie inclusă;

— evaluarea directivei ar trebui să se bazeze pe date cuprinzătoare, inclusiv pe numărul persoanelor care au fost efectiv condamnate – și nu doar urmărite penal – pe baza prelucrării datelor cu caracter personal.

58. În plus, AEPD recomandă ca evoluțiile privind PNR UE să fie evaluate într-o perspectivă mai amplă, care să includă evaluarea generală permanentă a tuturor instrumentelor UE în domeniul gestionării schimbului de informații lansate de către Comisie în ianuarie 2010. În cadrul evaluării necesității unui sistem UE PNR ar trebui avute în vedere în special rezultatele activităților în desfășurare privind modelul european de schimb de informații preconizat pentru 2012.

Adoptat la Bruxelles, 25 martie 2011.

Peter HUSTINX

Autoritatea Europeană pentru Protecția Datelor