

**Avizul Autorității Europene pentru Protecția Datelor privind Comunicarea Comisiei către Parlamentul European, Consiliu, Comitetul Economic și Social și Comitetul Regiunilor privind migrația**

(2012/C 34/02)

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 <sup>(1)</sup>,

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 <sup>(2)</sup>, în special articolul 41,

ADOPTĂ PREZENTUL AVIZ:

**I. INTRODUCERE**

1. La data de 4 mai 2011, Comisia a emis o Comunicare privind migrația <sup>(3)</sup> („comunicarea”). În conformitate cu articolul 41 din Regulamentul (CE) nr. 45/2001, Autoritatea Europeană pentru Protecția Datelor emite prezentul aviz din oficiu.
2. AEPD nu a fost consultată înainte de adoptarea comunicării. Acest lucru este regretabil, întrucât prezentarea observațiilor sale într-o etapă incipientă ar fi contribuit la soluționarea unora dintre problemele expuse în prezentul aviz.  
  
*Obiectivele și domeniul de aplicare al comunicării*
3. Comunicarea își propune să înscrie propunerile recente și viitoare de politici într-un cadru care ține cont de toate aspectele relevante ale migrației și să evite „o abordare pe termen scurt care să se limiteze la controlul la frontieră, fără a se lua în considerare aspectele pe termen lung” <sup>(4)</sup>. Comunicarea a fost redactată în principal ca răspuns la evenimentele actuale din Africa de Nord, în special la conflictul din Libia.
4. În acest scop, comunicarea se referă la ajutor umanitar, gestionarea frontierelor, vize, azil, nevoia economică de imigrație și integrare. Ea face trimitere la o serie de propuneri legislative, dintre care unele sunt noi, iar altele au fost deja prezentate. Multe dintre aceste propuneri vizează gestionarea frontierelor, aspect care ocupă o parte importantă a comunicării. Unele dintre acestea ar presupune o prelucrare pe scară largă a datelor cu caracter personal.
5. Comunicarea este doar prima dintr-o serie de comunicări și propuneri care urmează să fie emise în viitorul apropiat, fiecare prezentând în detaliu anumite aspecte la care se face referire în prezenta comunicare. În acest context, concluziile Consiliului European din 23 și 24 iunie 2011 <sup>(5)</sup> menționează

<sup>(1)</sup> JO L 281, 23.11.1995, p. 31.

<sup>(2)</sup> JO L 8, 12.1.2001, p. 1.

<sup>(3)</sup> COM(2011) 248 final.

<sup>(4)</sup> Comunicarea, p. 3.

<sup>(5)</sup> Concluziile Consiliului European din 23 și 24 iunie 2011, EUCO 23/11.

că aceste „eforturi vor fi consolidate și datorită accelerării lucrărilor cu privire la «frontierele inteligente», pentru a se asigura valorificarea noilor tehnologii în scopul soluționării problemelor legate de controlul frontierelor. În special, ar trebui introdus un sistem de intrare/ieșire și un program de înregistrare a pasagerilor. Consiliul European salută acordul obținut cu privire la Agenția pentru gestionarea operațională a unor sisteme informatice de mari dimensiuni în spațiul de libertate, securitate și justiție”.

#### Scopul avizului AEPD

6. Cu toate că aspectele privind protecția datelor nu reprezintă esența comunicării, aceasta menționează totuși mai multe inițiative și propuneri din domeniul gestionării frontierelor, precum sistemul de intrare/ieșire și programul de înregistrare a pasagerilor, care vor avea un impact semnificativ asupra dreptului fundamental la protecția datelor. În acest context, comunicarea subliniază contribuția majoră reprezentată de controlul la frontieră în lupta împotriva criminalității și face referire la Strategia de securitate internă prezentată de Comisie în 2010 <sup>(6)</sup>.
7. Multe dintre propunerile și inițiativele menționate urmează să fie prezentate mai detaliat în viitor; prin urmare, prezența comunicării oferă ocazia de a formula observații cu privire la aceste inițiative într-o etapă incipientă. Pentru inițiativele care au fost deja prezentate, precum propunerea de regulament de modificare a Regulamentului Frontex <sup>(7)</sup>, aceasta reprezintă o ocazie de a reitera unele dintre observațiile cele mai importante formulate anterior, înainte de adoptarea finală de către Consiliu și Parlamentul European.
8. Scopul prezentului aviz nu este acela de a analiza toate domeniile de politică vizate și toate propunerile menționate în comunicare, ci:
  - de a aborda mai multe principii și noțiuni privind protecția datelor, precum limitarea scopului, necesitatea, proporționalitatea și „luarea în considerare a vieții private începând cu momentul conceperii”, de care ar trebui să se țină cont la punerea în practică a abordării prezentate în comunicare;
  - de a discuta măsurile specifice propuse în comunicare din perspectiva protecției datelor și de a oferi încă din această etapă o consultare cu privire la modul în care se poate asigura respectarea corespunzătoare a drepturilor fundamentale, în special a dreptului la protecția datelor cu caracter personal.
9. În acest scop, avizul se compune din două părți principale. Prima parte cuprinde observații referitoare la abordarea generală adoptată în comunicare și considerații orizontale despre comunicare, precum necesitatea evaluării și implicațiile drepturilor fundamentale pentru felul în care sunt concepute sistemele informatice. Cea de a doua parte cuprinde observații care vizează propuneri și inițiative specifice <sup>(8)</sup>.

## II. OBSERVAȚII GENERALE

### Abordarea adoptată de comunicare

10. AEPD salută intenția comunicării de a evita „o abordare pe termen scurt care să se limiteze la controlul la frontieră, fără a se lua în considerare aspectele pe termen lung” <sup>(9)</sup>. O abordare cuprinzătoare și eficace a migrației nu poate consta doar în controlul la frontieră, ci trebuie să integreze și alte aspecte.

<sup>(6)</sup> Comunicarea Comisiei „Strategia de securitate internă a UE în acțiune: cinci pași către o Europă mai sigură”, COM(2010) 673.

<sup>(7)</sup> Propunere de regulament de modificare a Regulamentului (CE) nr. 2007/2004 al Consiliului de instituire a Agenției Europene pentru Gestionarea Cooperării Operative la Frontierele Externe ale Statelor Membre ale Uniunii Europene (Frontex), COM(2010) 61.

<sup>(8)</sup> Prezentul aviz utilizează și completează în mod special Avizul AEPD din 17 decembrie 2010 privind Comunicarea „Strategia de securitate internă în acțiune” („Avizul AEPD din 17 decembrie 2010”) (JO C 101, 1.4.2011, p. 6); Avizul AEPD din 15 decembrie 2010 cu privire la propunerea modificată de Regulament al Parlamentului European și al Consiliului privind instituirea sistemului „Eurodac” („Avizul AEPD din 15 decembrie 2010”) (JO C 101, 1.4.2011, p. 14); Avizul AEPD din 30 septembrie 2010 privind Comunicarea „Prezentare generală asupra modului de gestionare a informațiilor în spațiul de libertate, securitate și justiție” („Avizul AEPD din 30 septembrie 2010”) (JO C 355, 29.12.2010, p. 16); și Observațiile preliminare ale AEPD din 3 martie 2008 cu privire la „pachetul privind frontierele” („Observațiile preliminare ale AEPD din 3 martie 2008”), disponibile pe site-ul internet al AEPD.

<sup>(9)</sup> Comunicarea, p. 3.

11. O astfel de abordare cuprinzătoare trebuie să respecte drepturile fundamentale ale migranților și refugiaților, inclusiv dreptul la protecția datelor. Acest lucru este cu atât mai important, cu cât aceste grupuri se află deseori în situații de vulnerabilitate.
12. În acest context, comunicarea menționează faptul că obiectivul dual al Uniunii trebuie să fie menținerea unor niveluri ridicate de securitate și simplificarea, în același timp, a procedurilor de trecere a frontierei pentru „cei care ar trebui să fie admiși, cu respectarea deplină a drepturilor lor fundamentale”<sup>(10)</sup>. Această formulare ar putea crea impresia că nu este obligatoriu să se respecte și drepturile fundamentale ale persoanelor care – din diverse motive – nu ar trebui să fie admise. În opinia AEPD, este evident că drepturile acestora nu includ neapărat și dreptul de a se stabili pe teritoriul UE, caz în care s-ar impune reacții corespunzătoare, de exemplu operațiuni de returnare, însă întotdeauna cu respectarea drepturilor fundamentale.
13. Se constată că, din punctul de vedere al gestionării frontierelor, comunicarea pledează pentru o abordare care se bazează puternic pe utilizarea tehnologiei. Printre altele, aceasta este în favoarea unei supravegheri sporite la frontieră (a se vedea Sistemul european de supraveghere a frontierelor preconizat – Eurosur)<sup>(11)</sup>. De asemenea, comunicarea prevede explorarea posibilității de a institui sisteme informatice noi, la scară largă, pentru prelucrarea informațiilor despre pasageri (un sistem de intrare/ieșire și un program de înregistrare a pasagerilor)<sup>(12)</sup>. În cele din urmă, comunicarea pledează pentru extinderea sistemelor existente (respectiv Eurodac) la noi utilizatori<sup>(13)</sup>. Această concentrare asupra tehnologiei reflectă o tendință generală în ultimii ani.

*Evaluarea instrumentelor existente înainte de propunerea altora noi și testul necesității*

14. AEPD a subliniat de multe ori faptul că instrumentele existente ar trebui să fie evaluate înainte de a propune altele noi<sup>(14)</sup>. În acest context, amintind jurisprudența Curții Europene a Drepturilor Omului<sup>(15)</sup> și a Curții de Justiție a Uniunii Europene<sup>(16)</sup>, AEPD atrage atenția asupra faptului că interferențele cu dreptul la viață privată trebuie să corespundă standardului de a fi „necesare într-o societate democratică” și să respecte principiul proporționalității. Noțiunea de necesitate presupune o sarcină a probei mai strictă decât simpla „utilitate”<sup>(17)</sup>. Aceasta înseamnă că toate propunerile relevante trebuie să fie însoțite de o dovadă clară a necesității și proporționalității lor.
15. O astfel de dovadă trebuie oferită printr-o evaluare a impactului asupra vieții private<sup>(18)</sup>, elaborată pe baza unor dovezi suficiente<sup>(19)</sup>. O utilizare selectivă a statisticilor și a estimărilor nu este suficientă.

<sup>(10)</sup> Comunicarea, p. 7.

<sup>(11)</sup> Comunicarea, pp. 7 și 8 A se vedea și punctele 42-44 din prezentul aviz.

<sup>(12)</sup> Comunicarea, p. 10.

<sup>(13)</sup> Comunicarea, p. 14.

<sup>(14)</sup> A se vedea Avizul AEPD din 30 septembrie 2010, citat mai sus; a se vedea, de asemenea, Observațiile preliminare ale AEPD cu privire la „pachetul privind frontierele”, citate mai sus. În această privință, AEPD salută activitatea desfășurată de echipa de lucru responsabilă cu cartografierea informațiilor în contextul lucrului la modelul european de schimb de informații. Cu toate acestea, sfera de aplicare a acestui exercițiu ar trebui extinsă, iar activitatea viitoare în acest domeniu trebuie să adopte o perspectivă mai largă.

<sup>(15)</sup> A se vedea, de exemplu, Curtea Europeană a Drepturilor Omului, *S. și Marper/Regatul Unit*, cererile nr. 30562/04 și 30566/04, selectate pentru a fi publicate în *Recueil des arrêts et décisions*.

<sup>(16)</sup> De exemplu, cauzele conexe C-92/09 și C-93/09, *Volker und Markus Schecke și Hartmut Eifert/Land Hessen*, 2010, încă nepublicate în Raportul Curții Europene („Schecke”).

<sup>(17)</sup> Numeroase hotărâri ulterioare hotărârii Curții Europene a Drepturilor Omului în cauza *Handyside/United Kingdom*, 5493/72, seria A numărul 24, paragraful 48.

<sup>(18)</sup> Aceasta ar putea fi să ia forma unei evaluări separate a impactului asupra vieții private și a protecției datelor, fie să fie integrată în evaluarea generală a impactului. Orientările existente cu privire la evaluarea impactului [Orientările Comisiei Europene privind evaluarea impactului, SEC(2009) 92] nu prevăd o evaluare separată a impactului asupra drepturilor fundamentale, precum protecția datelor; aceste aspecte trebuie integrate în evaluarea generală a impactului. Între timp, ca urmare a Comunicării Comisiei privind strategia pentru punerea în aplicare efectivă a Cartei drepturilor fundamentale de către Uniunea Europeană [COM(2010) 573], au fost elaborate orientări suplimentare sub forma unui document de lucru al serviciilor Comisiei cu privire la orientările operaționale privind luarea în considerare a drepturilor fundamentale în cadrul analizelor de impact ale Comisiei [SEC(2011) 567].

<sup>(19)</sup> A se vedea și Avizul AEPD din 25 martie 2011 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 („Avizul AEPD din 25 martie 2011”), încă nepublicat în JO, în special punctul 25.

AEPD înțelege dificultatea culegerii de informații fiabile despre fenomene precum migrația ilegală; totuși, aceste evaluări ale impactului ar trebui să ia în considerare și soluții alternative la problemele întâlnite, pentru a reduce la minimum impactul asupra drepturilor fundamentale <sup>(20)</sup>. Simplul fapt că soluțiile tehnologice sunt fezabile nu înseamnă că ele sunt necesare și proporționale.

16. În cazul în care o evaluare conduce la concluzia că sunt necesare noi sisteme informatice la scară largă, la crearea acestora trebuie avut în vedere conceptul de „luare în considerare a vieții private începând cu momentul conceperii”. Operatorii trebuie să poată demonstra că la conceperea sistemelor s-au luat măsuri corespunzătoare pentru a se asigura respectarea cerințelor de confidențialitate. Acest lucru poate limita impactul negativ al noilor măsuri asupra vieții private (sau poate spori impactul pozitiv). Această abordare a fost avizată de către Comisie <sup>(21)</sup>. Punerea în practică a principiului „luării în considerare a vieții private începând cu momentul conceperii” în contextul unor sisteme precum sistemul de intrare/ieșire menționat în comunicare ar determina restricționarea culegerii de date cu caracter personal la minimumul necesar, limitând perioadele de păstrare și transformând prelucrarea datelor într-un proces transparent, care respectă confidențialitatea persoanelor vizate.
17. În plus, trebuie să se respecte și principiul limitării scopului, iar „denaturarea funcțiilor” trebuie prevenită. De exemplu, comunicarea prevede reintroducerea inițiativei de a acorda autorităților de aplicare a legii acces la sistemul Eurodac <sup>(22)</sup>, ceea ce pare să confirme existența unei tendințe de a acorda autorităților de aplicare a legii acces la sistemele UE la scară largă și ridică problema extinderii scopului inițial al sistemului. Acordarea accesului la bazele de date și altor autorități poate avea un impact grav: o bază de date considerată proporționată atunci când este utilizată pentru un singur scop specific poate deveni disproporționată atunci când utilizarea sa este extinsă ulterior la alte scopuri <sup>(23)</sup>.
18. În consecință, AEPD solicită ca toate propunerile (existente sau noi) care implică restricționări ale dreptului fundamental la protecția datelor să fie însoțite de o dovadă clară a necesității acestora <sup>(24)</sup>. De asemenea, atunci când sunt considerate necesare sistemele informatice la scară largă, ele trebuie concepute ținându-se cont în mod corespunzător de principiul „luării în considerare a vieții private începând cu momentul conceperii”. În plus, măsurile puse în aplicare trebuie să fie evaluate periodic pentru a se stabili dacă mai sunt necesare.

### III. OBSERVAȚII SPECIFICE

#### *Eurodac*

19. Comunicarea se referă la accesul autorităților de aplicare a legii la sistemul EURODAC, precizând că Eurodac, pe lângă faptul că va continua să sprijine eficiența Regulamentului Dublin, trebuie să „răspundă și altor nevoi ale autorităților de aplicare a legii” <sup>(25)</sup>.
20. Propunerea din decembrie 2008, care prevedea o reformare a Regulamentului Eurodac <sup>(26)</sup>, nu conținea dispoziții referitoare la accesul autorităților de aplicare a legii. Acestea au fost incluse într-o propunere

<sup>(20)</sup> Referitor la necesitatea luării în considerare a unor soluții alternative, a se vedea și hotărârea Curții de Justiție în cauza *Schecke*, citată mai sus.

<sup>(21)</sup> Comunicarea Comisiei referitoare la o abordare globală a protecției datelor cu caracter personal în Uniunea Europeană, COM(2010) 609, p. 12. A se vedea și Avizul AEPD din 14 ianuarie 2011 privind Comunicarea Comisiei către Parlamentul European, Consiliu, Comitetul Economic și Social și Comitetul Regiunilor – „O abordare globală a protecției datelor cu caracter personal în Uniunea Europeană” (JO C 181, 22.6.2011, p. 1), punctele 108-115.

<sup>(22)</sup> Comunicarea, p. 14.

<sup>(23)</sup> A se vedea Observațiile preliminare ale AEPD cu privire la „pachetul privind frontierele”, citate mai sus, p. 3.

<sup>(24)</sup> A se vedea și Avizul AEPD din 31 mai 2011 privind Raportul de evaluare al Comisiei către Consiliu și Parlamentul European referitor la Directiva privind păstrarea datelor (Directiva 2006/24/CE), încă nepublicat în JO, precum și Avizul AEPD din 25 martie 2011.

<sup>(25)</sup> Comunicarea, p. 14.

<sup>(26)</sup> Propunerea de Regulament privind instituirea sistemului „Eurodac” pentru compararea amprentelor digitale în scopul aplicării eficiente a Regulamentului (CE) nr. (.../...) (de stabilire a criteriilor și mecanismelor de determinare a statului membru responsabil de examinarea unei cereri de azil prezentate în unul dintre statele membre de către un resortisant al unei țări terțe sau de către un apatrid), COM(2008) 825.

înaintată de Comisie în septembrie 2009 <sup>(27)</sup>. În octombrie 2010, Comisia a adoptat o propunere modificată <sup>(28)</sup> care nu mai cuprinde dispoziții referitoare la accesul autorităților de aplicare a legii, la fel ca propunerea inițială.

21. În Avizul său din 15 decembrie 2010 privind sistemul Eurodac, AEPD a salutat omiterea accesului oferit autorităților de aplicare a legii <sup>(29)</sup>, amintind faptul că o astfel de utilizare în scop diferit trebuie să se bazeze pe dovezi substanțiale privind existența unei legături între solicitanții de azil și acte de terorism și/sau infracțiuni grave. În plus, atunci când se analizează necesitatea și proporționalitatea accesului trebuie să se țină cont și de situația precară a solicitanților de azil.
22. Reformarea Regulamentului Eurodac face parte din procesul de instituire a unui sistem european de azil, care, în conformitate cu Programul de la Stockholm, trebuie să aibă loc până în 2012 <sup>(30)</sup>. Unul dintre motivele menționate de Comisie pentru omiterea accesului autorităților de aplicare a legii în propunerea din octombrie 2010 a fost acela că neincluderea acestei măsuri controversate ar putea facilita adoptarea pachetului privind azilul în timp util <sup>(31)</sup>. Acest lucru are legătură și cu instituirea Agenției pentru gestionarea operațională a sistemelor informatice la scară largă în spațiul de libertate, securitate și justiție <sup>(32)</sup>.
23. În acest context și prin prisma observațiilor anterioare, poziția adoptată de AEPD este aceea că până în momentul de față nu au fost furnizate dovezi suficiente, clare și fiabile privind necesitatea reintroducerii accesului autorităților de aplicare a legii la sistemul Eurodac. Numai după o nouă evaluare a impactului, care să ia în considerare îngrijorările legate de viața privată, ar putea fi luată în calcul reintroducerea dispozițiilor respective. În plus, includerea accesului autorităților de aplicare a legii ar necesita modificări semnificative ale bazei de date Eurodac pentru a permite acest acces în condiții de securitate. Implicațiile tehnice și financiare ale acestui aspect ar trebui discutate, de asemenea, într-o nouă evaluare a impactului <sup>(33)</sup>.
24. În plus, reintroducerea propunerii ar putea avea un impact semnificativ asupra încadrării în timp a adoptării întregului pachet privind azilul. Comisia nu menționează o dată la care să fie prezentată o eventuală nouă propunere; de asemenea, nu menționează dacă o astfel de propunere ar fi însoțită de o nouă evaluare a impactului.

<sup>(27)</sup> Propunere modificată de Regulament al Parlamentului European și al Consiliului privind instituirea sistemului „Eurodac” pentru compararea amprentelor digitale în scopul aplicării eficiente a Regulamentului (CE) nr. (.../...) (de stabilire a criteriilor și mecanismelor de determinare a statului membru responsabil de examinarea unei cereri de protecție internațională prezentate în unul dintre statele membre de către un resortisant al unei țări terțe sau de către un apatrid), COM(2009) 342. AEPD a emis un aviz cu privire la această propunere – a se vedea Avizul AEPD din 7 octombrie 2009 cu privire la propunerea modificată de Regulament al Parlamentului European și al Consiliului privind instituirea sistemului „Eurodac” pentru compararea amprentelor digitale în scopul aplicării eficiente a Regulamentului (CE) nr. (.../...) (de stabilire a criteriilor și mecanismelor de determinare a statului membru responsabil de examinarea unei cereri de protecție internațională prezentate în unul dintre statele membre de către un resortisant al unei țări terțe sau de către un apatrid) și la propunerea de Decizie a Consiliului privind cererea autorităților de aplicare a legii din statele membre și a Europol de comparare a datelor Eurodac în scopul aplicării legii („Avizul AEPD din 7 octombrie 2009”) (JO C 92, 14.4.2010, p. 1).

<sup>(28)</sup> Propunere modificată de Regulament privind instituirea sistemului „Eurodac” pentru compararea amprentelor digitale în scopul aplicării eficiente a Regulamentului (CE) nr. (.../...) (de stabilire a criteriilor și mecanismelor de determinare a statului membru responsabil de examinarea unei cereri de protecție internațională prezentate în unul dintre statele membre de către un resortisant al unei țări terțe sau de către un apatrid), COM (2010) 555 [„COM(2010) 555”]. AEPD a emis un aviz cu privire la această propunere – a se vedea Avizul AEPD din 15 decembrie 2010, citat mai sus, în special punctele 18-22, 28-33, 51-57.

<sup>(29)</sup> Avizul AEPD din 15 decembrie 2010, în special punctele 12-17.

<sup>(30)</sup> Consiliul European; Programul de la Stockholm – O Europă deschisă și sigură în serviciul cetățenilor și pentru protecția acestora, p. 5 (JO C 115, 4.5.2010, p. 1).

<sup>(31)</sup> COM(2010) 555, citată mai sus, p. 3.

<sup>(32)</sup> Ibidem.

<sup>(33)</sup> Propunerea din octombrie 2010 nu a fost însoțită de o evaluare a impactului. În schimb, Comisia a făcut trimitere la evaluarea impactului realizată pentru propunerea din 2009 – a se vedea documentul de lucru al serviciilor Comisiei: Document de însoțire a propunerii modificate de Regulament al Parlamentului European și al Consiliului privind instituirea sistemului „Eurodac” pentru compararea amprentelor digitale în scopul aplicării eficiente a Regulamentului (CE) nr. (.../...) (de stabilire a criteriilor și mecanismelor de determinare a statului membru responsabil de examinarea unei cereri de protecție internațională prezentate în unul dintre statele membre de către un resortisant al unei țări terțe sau de către un apatrid), și a propunerii de decizie a Consiliului privind cererea autorităților de aplicare a legii din statele membre și a Europol de comparare a datelor Eurodac în scopul aplicării legii – Evaluarea impactului, SEC(2009) 936. A se vedea și COM(2010) 555, citată mai sus, p. 3.

*Sistemul de intrare/ieșire*

25. Comunicarea anunță și o comunicare privind frontierele inteligente, care urmează să fie emisă în septembrie 2011. Se presupune că această comunicare va discuta mai în detaliu inițiativele de creare a unui sistem de intrare/ieșire și a unui program de înregistrare a pasagerilor. Comisia recunoaște faptul că aceste proiecte ar necesita „investiții substanțiale” pentru a asigura „standarde ridicate pentru protecția datelor cu caracter personal”<sup>(34)</sup>.
26. În ceea ce privește sistemul de intrare/ieșire, Comisia justifică această inițiativă susținând că „șederile peste termen” reprezintă „principala sursă a imigrației ilegale în UE”<sup>(35)</sup>. În afară de această afirmație, comunicarea nu oferă nicio explicație cu privire la scopul sistemului respectiv.
27. Cu siguranță, reducerea numărului de „persoane care depășesc termenul legal de ședere” poate avea efecte pozitive. AEPD înțelege faptul că un sistem de intrare/ieșire ar descuraja șederea peste termen a resortisanților țărilor terțe, dacă aceștia știu că vor putea fi identificați în mod automat la expirarea vizei. Rămân totuși mai multe semne de întrebare.
28. Până în prezent nu există politici coerente cu privire la fenomenul șederii peste termen în statele membre. Conceptul de „ședere peste termen” nu este, în general, bine definit; agrearea unei definiții comune a termenului ar constitui un prim pas necesar către o înțelegere clară a problemei<sup>(36)</sup>.
29. În plus, toate cifrele vehiculate până în prezent reprezintă estimări<sup>(37)</sup>. Dimensiunea problemei ar trebui clarificată ca o condiție prealabilă a unei evaluări motivate a necesității.
30. Alertele emise în conformitate cu articolul 96 din Convenția de punere în aplicare a Acordului Schengen reprezintă una dintre măsurile existente de împiedicare a intrării anumitor persoane pe teritoriul Schengen. Aceste alerte pot fi utilizate pentru a preveni reintrarea persoanelor despre care se cunoaște că „au depășit termenul legal de ședere”<sup>(38)</sup>. Într-o comunicare recentă, Comisia a făcut apel la statele membre să utilizeze această posibilitate la maxim<sup>(39)</sup>. Acest lucru sugerează că măsura nu este utilizată în prezent la maxim.
31. Sistemul de intrare/ieșire s-ar baza, probabil, și pe date biometrice. Deși recunoaște eventualele avantaje ale utilizării datelor biometrice, AEPD se vede obligată să sublinieze și punctele slabe ale acesteia. Orice utilizare a datelor biometrice trebuie să fie însoțită de măsuri stricte de protecție și trebuie să țină cont de riscul producerii unor greșeli<sup>(40)</sup>. În acest context, AEPD încurajează instituirea unui set de criterii minime pentru utilizarea datelor biometrice, precum fiabilitatea datelor biometrice, evaluarea specifică a impactului datelor biometrice, precizia și o procedură de rezervă<sup>(41)</sup>. În plus, o anumită parte din

<sup>(34)</sup> Comunicarea, p. 10.

<sup>(35)</sup> Comunicarea, p. 10.

<sup>(36)</sup> De asemenea, ar fi necesar să se clarifice ce excepții s-ar aplica, de exemplu din motive medicale sau umanitare.

<sup>(37)</sup> A se vedea Avizul AEPD din 30 septembrie 2010, citat mai sus, punctele 52-56.

<sup>(38)</sup> A se vedea Observațiile preliminare ale AEPD din 3 martie 2008, citate mai sus, p. 4.

<sup>(39)</sup> Comunicarea Comisiei „Raport anual privind azilul”, COM(2011) 291, p. 9.

<sup>(40)</sup> A se vedea, de exemplu, Avizul AEPD din 16 octombrie 2006 privind propunerea modificată de regulament al Consiliului de modificare a Regulamentului (CE) nr. 1030/2002 de instituire a unui model uniform de permis de ședere pentru resortisanții țărilor terțe (JO C 320, 28.12.2006, p. 21); a se vedea și Avizul nr. 3/2007 al Grupului de lucru pentru protecția persoanelor în ceea ce privește prelucrarea datelor cu caracter personal privind propunerea de regulament al Parlamentului European și al Consiliului de modificare a Instrucțiunilor consulare comune privind vizele adresate misiunilor diplomatice și oficiilor consulare în legătură cu introducerea biometriei, inclusiv a dispozițiilor privind organizarea primirii și prelucrării cererilor de viză [COM(2006) 269 final], WP134 din 1 martie 2007.

<sup>(41)</sup> A se vedea, de exemplu, Avizul AEPD din 19 octombrie 2005 privind propunerea de Decizie a Consiliului privind instituirea, funcționarea și utilizarea Sistemului de informații Schengen din a doua generație (SIS II), propunerea de Regulament al Parlamentului European și al Consiliului privind instituirea, funcționarea și utilizarea Sistemului de informații Schengen din a doua generație [...] (JO C 91, 19.4.2006 p. 38); și „Către o protecție a datelor mai cuprinzătoare în Europa, incluzând datele biometrice – Perspectiva europeană”, a douăsprezecea conferință a Institutului de Biometrie din Australia, Sydney, 26 mai 2011:  
[http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2011/11-05-26\\_Biometrics\\_Institute\\_EN.pdf](http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2011/11-05-26_Biometrics_Institute_EN.pdf)

populația vizată nu are amprente care să poată fi citite de un astfel de sistem<sup>(42)</sup>. Dacă sistemul de intrare/ieșire urmează să includă date biometrice, ar trebui prevăzute proceduri de rezervă pentru acești pasageri<sup>(43)</sup>.

32. AEPD dorește, de asemenea, să atragă atenția asupra experiențelor înregistrate în legătură cu US-VISIT (Tehnologia de indicare a statutului imigranților și vizitatorilor din Statele Unite), un sistem similar din SUA. În cadrul US-VISIT, majoritatea resortisanților țărilor terțe sunt obligați să furnizeze date biometrice la intrarea pe teritoriul Statelor Unite. Partea de „ieșire” a acestui sistem este încă în curs de elaborare. În 2009 au fost efectuate două teste-pilot privind culegerea de date biometrice pentru această parte a sistemului<sup>(44)</sup>. Departamentul de Securitate Internă (*Department of Homeland Security*) a recunoscut faptul că rezultate acestor teste sunt „amplificate de unele limitări ale sistemului, legate de situațiile în care evidențele ADIS nu reflectau statutul actualizat al pasagerului din cauza unor modificări recente sau prelungiri ale statutului”<sup>(45)</sup>. De asemenea, testele au inclus filtrarea pasagerilor pe baza mai multor liste de persoane aflate sub supraveghere; cu toate acestea, „niciunul dintre [...] rezultate nu ar fi împiedicat plecarea”<sup>(46)</sup>. În total, Departamentul de Securitate Internă a cheltuit aproximativ 1,3 miliarde USD pentru elaborarea componentei de intrare a sistemului US-VISIT<sup>(47)</sup>. Acest lucru naște întrebarea dacă un sistem de intrare/ieșire este o măsură de reducere a „șederilor peste termen” eficientă din punctul de vedere al costurilor.
33. Pe scurt, nici scopul unui astfel de sistem, nici modul în care ar fi construit și aplicat acesta nu sunt suficient de clare. În ceea ce privește nevoia de a lua măsuri, nu există o definiție clară a noțiunii centrale de „ședere peste termen”; în consecință, nu există statistici fiabile care să reflecte dimensiunea problemei. Cu privire la măsurile ce trebuie adoptate, instrumentele existente de prevenire a reintrării persoanelor despre care se cunoaște că „au depășit termenul legal de ședere” nu sunt, probabil, utilizate în măsura necesară; în plus, componenta biometrică a sistemului de intrare/ieșire ridică semne de întrebare. În ceea ce privește fezabilitatea și costurile acestui sistem, experiențele din SUA arată că implementarea unui sistem de intrare/ieșire va fi costisitoare. Aceste aspecte proiectează îndoieli asupra necesității și eficienței sistemului de intrare/ieșire din punctul de vedere al costurilor.

#### *Programul de înregistrare a pasagerilor*

34. Comunicarea mai menționează și introducerea unui program de înregistrare a pasagerilor. Nu este absolut clar care ar fi valoarea adăugată a acestui sistem prin comparație, de exemplu, cu utilizarea unei vize cu intrări multiple cu o perioadă îndelungată de valabilitate. Grupurile-țintă ar fi aceleași (persoanele care călătoresc frecvent). Faptul că există încă „reticență”<sup>(48)</sup> față de eliberarea unor astfel de vize nu poate constitui, în sine, un motiv suficient pentru propunerea unor măsuri noi, atâta vreme cât cele existente în prezent ar permite – dacă ar fi utilizate în totalitatea lor – atingerea aceluiași obiective. Prin prisma celor menționate mai sus, AEPD nu este pe deplin convinsă că sistemul este cu adevărat necesar.
35. În plus, comunicarea se referă la conceptul de călători „bona fide” (pagina 11), îndeosebi în legătură cu programul de înregistrare a pasagerilor. Implicit, s-ar putea interpreta că această formulare creează o

<sup>(42)</sup> Acest lucru se poate datora, de exemplu, unor boli, handicapuri, răni sau arsuri. De asemenea, se pare că un număr semnificativ de persoane care lucrează în agricultură și construcții au amprente atât de degradate, încât sunt aproape ilizibile. A se vedea și Avizul AEPD din 15 decembrie 2010, citat mai sus, punctul 19.

<sup>(43)</sup> Pentru observații similare în contextul Eurodac, a se vedea Avizul AEPD din 15 decembrie 2010, punctele 18-25.

<sup>(44)</sup> La unul dintre aeroporturile selectate pentru testare, costurile forței de muncă și cheltuielile au însumat 393 410 USD pentru 35 de zile de operațiuni de testare, ca rezultat înregistrându-se 90 de cazuri suspectate de „ședere peste termen”. La un al doilea test efectuat în același timp au rezultat 44 de cazuri suspectate, cu un cost de 77 501 USD. Aceste cifre nu includ costurile de dezvoltare. Pentru o analiză a acestor teste, a se vedea studiul întocmit de *United States Government Accountability Office* (Corpul de Control al Administrației Statelor Unite), intitulat *US-VISIT Pilot Evaluations Offer Limited Understanding of Air Exit Options* (Evaluările-pilot ale US-VISIT oferă o înțelegere limitată a opțiunilor de ieșire pe cale aeriană), august 2010, GAO-10-860, document disponibil la: <http://www.gao.gov/new.items/d10860.pdf> („GAO SUA: Evaluări-pilot ale US-VISIT”).

<sup>(45)</sup> Reproducere din US GAO: Evaluări-pilot ale US-VISIT, p. 72.

<sup>(46)</sup> US GAO: Evaluări-pilot ale US-VISIT, p. 72.

<sup>(47)</sup> A se vedea Observațiile preliminare ale AEPD din 3 martie 2008, citate mai sus, p. 4.

<sup>(48)</sup> Comunicarea, p. 11.

categorie de călători „mala fide”. Numai călătorii care întreprind acțiuni suplimentare, înscriindu-se în programul de înregistrare a pasagerilor și furnizând informații personale adiționale, ar fi considerați „bona fide”. În acest caz nu s-ar mai pleca de la ipoteza conform căreia, în general, călătorii care intră în Uniune trebuie să fie considerați de bună-credință, cu excepția situației în care anumite dovezi ridică suspiciuni, ci de la aceea că este obligația călătorilor să se discolpe furnizând informații suplimentare despre ei înșiși, chiar și în absența oricăror dovezi. Implicația este că, dacă doar unii dintre călători sunt declarați a fi „bona fide”, cei care nu sunt dispuși să ofere informații suplimentare intră de fapt în categoria „mala fide”, deși refuzul de a furniza informații suplimentare poate avea motive întemeiate, de exemplu faptul că persoanele respective nu călătoresc frecvent <sup>(49)</sup>.

#### *Frontex și cooperarea între agenții*

36. Comunicarea face apel la o „cooperare strânsă între agenții” (Europol, FRONTEX și autoritățile vamale și polițienești naționale), considerată „esențială”, mai ales între autoritățile de control la frontieră și autoritățile vamale <sup>(50)</sup>. Această cooperare va fi susținută prin propunerile de bune practici care urmează să fie prezentate în cursul anului 2012. De asemenea, Comisia anunță o propunere legislativă care urmează să fie prezentată în cursul anului 2011 și care va permite agențiilor statelor membre care efectuează activități de supraveghere a frontierei „să facă schimb de informații operaționale și să coopereze între ele și cu agenția Frontex” <sup>(51)</sup>. În cele din urmă, propunerea de actualizare a cadrului juridic al Frontex pentru a fi „mai eficace din punct de vedere al capacității sale operative” este negociată în prezent în Consiliu și Parlamentul European <sup>(52)</sup>.
37. În vederea asigurării coerenței și a creării de valoare adăugată din perspectiva protecției datelor, dispozițiile corespunzătoare din temeiurile juridice pentru încheierea unor eventuale acorduri de cooperare și schimburi de date cu caracter personal între Frontex și agențiile cu care aceasta urmează să coopereze trebuie să fie coerente și consecvente pentru a asigura cooperarea deplină între organisme în privința normelor privind protecția datelor.
38. AEPD reiterează încă o dată aspectele menționate în Avizul său privind propunerea de reformare a Regulamentului Frontex <sup>(53)</sup>, în special necesitatea existenței unui temei juridic clar pentru prelucrarea datelor cu caracter personal. Dacă Frontex primește mandatul de a face schimb de date cu caracter personal, acesta trebuie să cuprindă dispoziții ferme și clare referitoare la drepturile persoanelor vizate, precum și alte măsuri de protecție. Orice dispoziție care permite Frontex să prelucreze și/sau să facă schimb de date cu caracter personal trebuie să fie precisă și clar delimitată.

#### *Eurosur*

39. Comisia mai anunță, pentru luna decembrie 2011, o propunere legislativă care să definească domeniul de aplicare, scopul și cadrul tehnic și operațional al Sistemului european de supraveghere a frontierelor (Eurosur) <sup>(54)</sup>. Se presupune că această propunere va asigura „o utilizare mai intensă a tehnologiilor moderne la frontierele terestre, precum și la frontierele maritime” <sup>(55)</sup>, precum și schimbul de informații operaționale cu privire la orice incident <sup>(56)</sup>. Acest aspect are legătură și cu Frontex, întrucât Comisia intenționează să prezinte o altă propunere care să permită autorităților statelor membre care efectuează activități de supraveghere a frontierei să facă schimb de informații operaționale între ele și cu agenția Frontex <sup>(57)</sup>.

<sup>(49)</sup> A se vedea și Observațiile preliminare ale AEPD din 3 martie 2008, citate mai sus.

<sup>(50)</sup> Comunicarea, p. 10.

<sup>(51)</sup> Comunicarea, p. 8.

<sup>(52)</sup> Comunicarea, p. 8.

<sup>(53)</sup> Avizul AEPD din 17 mai 2010 privind propunerea de regulament al Parlamentului European și al Consiliului de modificare a Regulamentului (CE) nr. 2007/2004 al Consiliului de instituire a Agenției Europene pentru Gestionarea Cooperării Operative la Frontierele Externe ale Statelor Membre ale Uniunii Europene (Frontex), încă nepublicat în JO; a se vedea și Avizul AEPD din 17 decembrie 2010, citat mai sus, punctele 48-51.

<sup>(54)</sup> Comunicarea, p. 18.

<sup>(55)</sup> Comunicarea, p. 7.

<sup>(56)</sup> Comunicarea, p. 8.

<sup>(57)</sup> Comunicarea, p. 8.



40. Nu este clar dacă și în ce măsură aceasta ar include și prelucrarea datelor cu caracter personal <sup>(58)</sup>. AEPD îndeamnă Comisia să clarifice aceste aspecte în propunerile care vor urma.

*Sistemul european al polițiștilor de frontieră*

41. Comunicarea menționează faptul că ar trebui analizată fezabilitatea unui sistem european al polițiștilor de frontieră. Nu se desprinde clar din text cum ar arăta acest sistem. Conform textului, acesta nu ar trebui „în mod necesar” <sup>(59)</sup> să presupună o administrație centrală, ceea ce lasă deschisă posibilitatea ca aceasta să existe totuși. Dacă nu urmează să existe o administrație centrală, Comisia sugerează că trebuie îmbunătățite, printre altele, „capacitățile comune” și „cooperarea practică” <sup>(60)</sup>.
42. Nu este clar dacă acest lucru este menit să vizeze o mai bună punere în aplicare a măsurilor existente sau dacă este o aluzie la alte propuneri, care nu au fost încă anunțate. Dat fiind faptul că „cooperarea practică” ar putea să includă și schimburi de date cu caracter personal, pentru care trebuie să existe în mod cert un temei juridic, acest lucru ar trebui să fie precizat în propunerile viitoare, dacă se va da curs proiectului.

#### IV. CONCLUZIE ȘI RECOMANDĂRI

43. În concordanță cu jurisprudența constantă a Curții de Justiție a Uniunii Europene și a Curții Europene a Drepturilor Omului, AEPD amintește cerința referitoare la necesitate și proporționalitate în ceea ce privește toate propunerile (existente și noi) care încalcă drepturile fundamentale la viață privată și la protecția datelor. Pentru fiecare propunere, necesitatea trebuie demonstrată printr-o evaluare a impactului asupra vieții private.
44. Atunci când se propun și se concep noi sisteme informatice la scară largă trebuie să se respecte principiul „luării în considerare a vieții private începând din momentul conceperii” și principiul limitării scopului.
45. AEPD insistă ca orice utilizare a datelor biometrice să fie însoțită de măsuri stricte de protecție și de proceduri de rezervă pentru cei care nu se pot înregistra. În termeni mai generali, trebuie stabilite condiții minime pentru utilizarea datelor biometrice.
46. În plus, AEPD îndeamnă Comisia să clarifice domeniul de aplicare și conținutul propunerilor sale menționate în prezentul aviz. Acest lucru este valabil pentru propunerile legislative anunțate referitoare la sistemul de intrare/ieșire, programul de înregistrare a pasagerilor, EUROSUR, FRONTEX și cooperarea între agenții, precum și pentru comunicarea privind frontierele inteligente și studiul cu privire la un sistem european al polițiștilor de frontieră.
47. De asemenea, AEPD solicită Comisiei să nu reintroducă propunerea privind accesul autorităților de aplicare a legii la sistemul Eurodac, cu excepția cazului în care o nouă evaluare a impactului ar demonstra în mod clar necesitatea propunerii, inclusiv implicațiile tehnice și financiare pentru sistem.
48. AEPD va urmări îndeaproape aceste evoluții și va formula observații suplimentare, dacă va fi cazul. AEPD este disponibilă pentru consultări ulterioare, în spiritul bunei cooperări.

Adoptat la Bruxelles, 7 iulie 2011.

Peter HUSTINX

Autoritatea Europeană pentru Protecția Datelor

---

<sup>(58)</sup> A se vedea și Avizul AEPD din 17 decembrie 2010, citat mai sus, punctele 46 și 47, care a abordat deja această chestiune. Prezentul aviz abordează și problema, nerezolvată până în prezent, a naturii legăturilor preconizate dintre Frontex și Eurosur.

<sup>(59)</sup> Comunicarea, p. 7.

<sup>(60)</sup> Comunicarea, p. 7.