

## I

(Rezoluții, recomandări și avize)

## AVIZE

## AUTORITATEA EUROPEANĂ PENTRU PROTECȚIA DATELOR

**Avizul Autorității Europene pentru Protecția Datelor 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 într-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**

(2010/C 92/01)

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 <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,

având în vedere solicitarea de aviz formulată în conformitate cu articolul 28 alineatul (2) din Regulamentul (CE) nr. 45/2001 primită la 15 septembrie 2009 din partea Comisiei Europene,

ADOPTĂ PREZENTUL AVIZ:

### I. INTRODUCERE

1. La 10 septembrie 2009 Comisia a adoptat două propuneri, și anume: 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 într-unul dintre statele membre de către un resortisant al unei țări terțe sau de către un apatrid) <sup>(3)</sup> și 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 <sup>(4)</sup>. Propunerile au fost transmise de către Comisie AEPD spre consultare și au fost primite la 15 septembrie 2009, în conformitate cu articolul 28 alineatul (2) din Regulamentul (CE) nr. 45/2001 (denumite în continuare „propunerile” sau „regulamentul propus” și „decizia propusă”). AEPD a primit, de asemenea, evaluarea impactului.

2. AEPD salută faptul că este consultată și recomandă ca trimiterea la această consultare să fie făcută în considerentele propunerii, de manieră similară ca într-un număr de alte texte legislative cu privire la care AEPD a fost consultată, în conformitate cu Regulamentul (CE) nr. 45/2001.

3. AEPD are un interes specific cu privire la aceste propuneri și în lumina competențelor de supraveghere pe care le exercită asupra bazei de date a unității centrale Eurodac, precum și a supravegherii coordonate pe care trebuie să o asigure asupra sistemului Eurodac în ansamblul său împreună cu autoritățile naționale pentru protecția datelor.

<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(2009) 342 final.

<sup>(4)</sup> COM(2009) 344 final.

4. Aspectul legat de oferirea accesului la sistemele informatice de mari dimensiuni pentru aplicarea legii a fost deja abordat de către AEPD în contextul accesului la Sistemul de Informații privind Vizele de către autoritățile de aplicare a legii și Europol<sup>(5)</sup>. Obiectul propunerilor este legat îndeaproape și de reformarea generală a regulamentelor Eurodac și Dublin cu privire la care AEPD a emis două avize la 18 februarie 2009<sup>(6)</sup>.

## II. CONȚINUTUL ȘI CONTEXTUL PROPUNERILOR

5. Propunerile stabilesc bazele corespunzătoare dreptului autorităților desemnate ale statelor membre, precum și al Europol de a solicita o comparare a datelor dactiloscopice sau o copie latentă cu datele Eurodac. O comparare reușită care generează un rezultat pozitiv din partea Eurodac va fi însoțită de toate datele deținute de Eurodac cu privire la amprenta digitală. Solicitățile de informații suplimentare ca urmare a unui rezultat pozitiv nu sunt reglementate în propuneri, dar sunt acoperite de instrumentele existente aferente schimbului de informații privind respectarea legii. Domeniul de aplicare al propunerilor acoperă lupta împotriva infracțiunilor cu caracter terorist și a infracțiunilor grave, precum traficul de ființe umane și de droguri<sup>(7)</sup>.

6. Articolul 7 al deciziei propuse determină condițiile de accesare a datelor Eurodac de către autoritățile desemnate. Accesul este permis doar dacă se obțin rezultate negative la compararea bazelor de date dactiloscopice naționale și a bazelor de date dactiloscopice automatizate ale altor state membre în temeiul Deciziei 2008/615/JAI a Consiliului privind intensificarea cooperării transfrontaliere, în special în domeniul combaterii terorismului și a criminalității transfrontaliere<sup>(8)</sup> și dacă compararea este necesară pentru combaterea infracțiunilor cu caracter terorist sau a altor infracțiuni grave, atunci când compararea este necesară într-un caz specific și dacă există motive întemeiate pentru a considera că o astfel de comparare va contribui în mod substanțial la combaterea oricăreia din infracțiunile în cauză. AEPD ia act de faptul că articolul 7 nu impune ca persoana vizată, ale cărei amprente digitale fac obiectul cererii, să fie suspectată de vreuna din respectivele infracțiuni.

<sup>(5)</sup> Avizul din 20 ianuarie 2006 cu privire la propunerea de decizie a Consiliului privind accesul la Sistemul de informații privind vizele, în vederea consultării de către autoritățile statelor membre responsabile cu securitatea internă și de către Europol în scopul prevenirii, detectării și investigării infracțiunilor de terorism și a altor infracțiuni grave [COM (2005) 600 final], JO C 97, 25.4.2006, p. 6.

<sup>(6)</sup> Avizul din 18 februarie 2009 cu privire la 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 protecție internațională prezentate într-unul dintre statele membre de către un resortisant al unei țări terțe sau de către un apatrid) [COM(2008) 825] și avizul din 18 februarie 2009 cu privire la propunerea de regulament de stabilire a criteriilor și mecanismelor de determinare a statului membru responsabil de examinarea unei cereri de azil prezentate într-unul dintre statele membre de către un resortisant al unei țări terțe sau un apatrid [COM(2008) 820 final].

<sup>(7)</sup> A se vedea în special articolul 1 al deciziei propuse.

<sup>(8)</sup> JO L 210, 6.8.2008, p. 1, denumită în continuare: Decizia Prüm.

7. Ar trebui reamintit faptul că obiectivul creării sistemului Eurodac a fost facilitarea aplicării Regulamentului Dublin, care face posibilă identificarea statelor membre responsabile cu examinarea cererilor de azil, prin compararea amprentelor digitale ale solicitanților de azil și ale imigranților ilegali. Sistemul Eurodac permite statelor membre să identifice solicitanții de azil și persoanele care au fost reținute în timpul trecerii ilegale a unei frontiere externe a Comunității. Prin compararea amprentelor digitale, statele membre pot determina dacă un solicitant de azil sau un cetățean străin aflat ilegal pe teritoriul unui stat membru a solicitat anterior azil în alt stat membru sau dacă un solicitant de azil a pătruns ilegal pe teritoriul Uniunii. La adoptare, regulamentul privind instituirea Eurodac nu a prevăzut accesul poliției la Eurodac; amprentele digitale erau colectate în scopul foarte specific descris la articolul 1 alineatul (1) din Regulamentul Eurodac.

8. Articolul 1 alineatul (2) din regulamentul propus extinde scopul sistemului Eurodac și adaugă scopul prevenirii, depistării și anchetării infracțiunilor cu caracter terorist și a altor infracțiuni grave, în condițiile prezentate în propuneri. Această modificare a scopului este explicată în considerentul (6) din decizia propusă care stipulează următoarele: „Deoarece Eurodac a fost instituit pentru a facilita aplicarea Regulamentului Dublin, accesul la Eurodac în scopul prevenirii, detectării sau anchetării infracțiunilor cu caracter terorist și a altor infracțiuni grave constituie o modificare a scopului inițial al Eurodac, care afectează dreptul la respectarea vieții private a persoanelor ale căror date cu caracter personal sunt prelucrate în Eurodac.”

9. Accesarea Eurodac de către autoritățile de aplicare a legii a fost deja anunțată în trecut, la câțiva ani de la adoptarea Regulamentului Eurodac. În documente precum Programul de la Haga, concluziile Comitetului mixt al Consiliului JAI din 12-13 iunie 2007 și Comunicarea Comisiei către Consiliu și către Parlamentul European din 24 noiembrie 2005<sup>(9)</sup> privind îmbunătățirea eficienței, creșterea interoperabilității și a sinergiilor dintre bazele de date la nivel european în domeniul justiției și al afacerilor interne, se menționează următoarele: „În legătură cu obiectivul de combatere a terorismului și a criminalității, Consiliul identifică în prezent lipsa posibilității de accesare de către autoritățile de securitate internă a datelor VIS ca pe o deficiență. Același lucru poate fi spus referitor la datele privind imigrația conținute în SIS II și la datele Eurodac.”

10. Astfel cum a fost recunoscut atât în evaluarea impactului, cât și în expunerea de motive, propunerile de a oferi accesul la Eurodac autorităților de aplicare a legii au provocat critici semnificative din partea mai multor părți interesate.

<sup>(9)</sup> COM(2005) 597 final, punctul 4.6.

### III. SCOPUL AVIZULUI

11. În prezentul aviz, AEPD va analiza legitimitatea propunerilor. Această analiză va conduce la concluzia că AEPD are îndoieli serioase referitoare la legitimitatea propunerilor și la oportunitatea adoptării instrumentelor legislative pe baza acestor propuneri.

12. Analiza va fi realizată pe baza următoarelor etape:

(a) punctul de plecare: Cum să se asigure echilibrul corect între necesitatea de securitate publică și dreptul la protecția datelor;

(b) propunerile ca o continuare a două tendințe mai generale:

(i) autoritățile de aplicare a legii beneficiază din ce în ce mai mult de facilitatea de a utiliza datele cu caracter personal ale persoanelor fizice care nu sunt legate în mod direct de o infracțiune specifică și care au fost colectate în alte scopuri;

(ii) au fost propuse instrumente juridice noi în plus față de instrumentele juridice existente, care nu au fost încă puse în aplicare pe deplin. Acest fapt ridică întrebări referitoare la necesitatea unor asemenea instrumente noi;

(c) circumstanțele specifice ale cazului prezent. O mare cantitate de informații este deja disponibilă pentru autoritățile de aplicare a legii în acest domeniu;

(d) propunerea va avea impact în special asupra unui grup particular vulnerabil la nivelul societății, și anume solicitanții de azil, cu riscul de a stigmatiza în continuare acest grup;

(e) calendarul propunerilor. Propunerile sunt adoptate, fără să se aștepte două modificări importante de context care ar putea avea un impact important asupra propunerilor, și anume Programul de la Stockholm și intrarea (posibilă) în vigoare a Tratatului de la Lisabona. De asemenea, propunerea este făcută independent de reformarea generală a regulamentelor Eurodac și Dublin, care este încă discutată în cadrul Consiliului și al Parlamentului European;

(f) compatibilitatea cu articolul 8 din Convenția europeană a drepturilor omului.

13. Avizul nu va analiza în detaliu prevederile de fond ale propunerilor. În general, calitatea legislativă a prevederilor este bună. Acestea sunt bine formulate și asigură condiții stricte în temeiul cărora autoritățile desemnate ale statelor membre și Europol pot solicita compararea datelor dacti-

loscopice cu cele stocate în baza de date centrală Eurodac. Cu toate acestea, la punctele 49-50 vor fi formulate câteva comentarii cu privire la fond.

### IV. PUNCTUL DE PLECARÉ

14. AEPD dorește să evidențieze că un schimb de informații mai bun reprezintă un obiectiv politic esențial pentru Uniunea Europeană. Punerea unui accent pe schimbul de informații este și mai logică în absența unei forțe de poliție europene, a unui sistem de justiție penală european și a unui control european la frontiere complet armonizat. Măsurile referitoare la informații reprezintă, prin urmare, o contribuție esențială a Uniunii Europene, care permite autorităților naționale ale statelor membre să abordeze criminalitatea transfrontalieră și să protejeze frontierele externe de manieră eficientă. Totuși, acestea ar trebui să contribuie nu numai la securitatea cetățenilor, ci și la apărarea libertăților fundamentale ale acestora.

15. Cu alte cuvinte, guvernele au nevoie de instrumente adecvate pentru a garanta securitatea cetățenilor, dar acestea trebuie să respecte pe deplin la nivelul societății noastre europene drepturile fundamentale ale cetățenilor. Este sarcina legislatorului UE să asigure acest echilibru. Necesitatea unui asemenea echilibru este evidențiată explicit de către Comisie în comunicarea sa din 10 iunie 2009 intitulată „Un spațiu de libertate, securitate și justiție în serviciul cetățenilor”<sup>(10)</sup>. Acesta joacă, de asemenea, un rol important în cadrul discuțiilor privind un nou program multianual în domeniul libertății, securității și justiției („Programul de la Stockholm”).

16. Este bine să se evidențieze în acest context faptul că dreptul aplicabil protecției datelor nu prejudiciază în niciun fel interesele legitime ale guvernelor de a proteja securitatea publică. Dacă datele sunt necesare într-un scop specific și legitim, acestea pot fi utilizate, acolo unde este necesar, cu luarea de măsuri suplimentare care prevăd garanții adecvate. Este, de asemenea, esențial ca informațiile să fie culese, partajate și prelucrate numai pe baza unor nevoi concrete de securitate și luând în considerare principiile protecției datelor.

17. Lupta împotriva infracțiunilor cu caracter terorist și a altor infracțiuni grave<sup>(11)</sup> poate reprezenta cu certitudine un motiv legitim pentru a permite prelucrarea datelor cu caracter personal, în conformitate cu drepturile fundamentale la viață privată și la 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. Acest lucru este necesar în mai mare măsură în cazul unei imixtiuni extinse în drepturile persoanelor fizice care constituie un grup vulnerabil care necesită protecție, astfel cum este prevăzut în propuneri.

<sup>(10)</sup> COM(2009) 262 final. A se vedea de asemenea avizul AEPD din 10 iulie 2009 privind această comunicare, punctul 22.

<sup>(11)</sup> Scopurile în care este permisă compararea datelor dactiloscopice în temeiul articolului 1 din decizia propusă.

## V. CONTINUAREA UNOR TENDINȚE MAI GENERALE

*Tendința de a acorda autorităților de aplicare a legii un acces larg la date*

18. Ar trebui subliniat faptul că propunerile nu numai că se încadrează în tendința generală de a acorda autorităților de aplicare a legii acces la câteva sisteme de informații și de identificare de mari dimensiuni, dar constituie, de asemenea, un pas înainte într-o tendință de a acorda autorităților de aplicare a legii accesul la date ale persoanelor fizice care în principiu nu sunt suspectate de a fi comisoare infracțiuni. Acest lucru se referă, de asemenea, la datele care au fost colectate în scopuri care nu au legătură cu combaterea criminalității. Exemple recente:

— Directiva 2006/24/CE a Parlamentului European și a Consiliului din 15 martie 2006 privind păstrarea datelor generate sau prelucrate în legătură cu furnizarea serviciilor de comunicații electronice accesibile publicului sau de rețele de comunicații publice și de modificare a Directivei 2002/58/CE <sup>(12)</sup>;

— Decizia 2008/633/JAI a Consiliului din 23 iunie 2008 privind accesul la Sistemul de informații privind vizele (VIS) în vederea consultării de către autoritățile desemnate ale statelor membre și de către Europol în scopul prevenirii, depistării și cercetării infracțiunilor de terorism și a altor infracțiuni grave <sup>(13)</sup>;

— Propunere de decizie-cadru a Consiliului privind utilizarea registrului cu numele pasagerilor (PNR) în scopul aplicării legii <sup>(14)</sup>.

19. În opiniile sale referitoare la aceste inițiative, AEPD a avut o abordare critică în ceea ce privește acordarea autorităților de aplicare a legii a accesului la datele cu caracter personal ale persoanelor fizice care nu sunt suspectate de săvârșirea vreunei infracțiuni și care au fost colectate în alte scopuri. AEPD subliniază necesitatea de a formula o justificare adecvată și de îndeplini cerințele de necesitate și proporționalitate. În avizul său privind PRN, autoritatea a prevenit cu privire la trecerea la o societate de supraveghere totală.

<sup>(12)</sup> JO L 105, 13.4.2006, p. 54. Avizul AEPD din 26 septembrie 2005, JO C 298, 29.11.2005, p. 1.

<sup>(13)</sup> JO L 218, 13.8.2008, p. 129.

<sup>(14)</sup> Neadoptat încă de către Consiliu; ultima versiune disponibilă în registrul Consiliului din 29 iunie 2009, 5618/2/09. Avizul AEPD din 20 decembrie 2007, JO C 110, 1.5.2008, p. 1.

20. Această abordare a fost menționată în avizul AEPD privind Comunicarea Comisiei din 10 iunie 2009 intitulată „Un spațiu de libertate, securitate și justiție în serviciul cetățenilor” <sup>(15)</sup>. Avizul invită la abordarea specifică în cadrul Programului de la Stockholm a tendinței de a utiliza informațiile colectate în alte scopuri. Sunt necesare condiții stricte, precum condiția potrivit căreia solicitările de date ar trebui să fie proporționale, strict direcționate și, în principiu, bazate pe suspiciuni cu privire la persoane specifice.

*Necesitatea unei dezbateri generale privind accesul în scopul aplicării legii*

21. Prezentul aviz trebuie văzut și în contextul unei dezbateri mai largi cu privire la viitorul schimbului de informații la nivelul UE și al tendinței crescute a accesului în scopul aplicării legii la baze de date enorme. AEPD profită de această oportunitate pentru a sublinia necesitatea unei evaluări de la caz la caz a fiecărei propuneri de acest fel și a unei viziuni coerente, cuprinzătoare și orientate către viitor asupra acestui subiect, preferabil în legătură cu Programul de la Stockholm.

22. În prezent, mai mult ca înainte, este necesară de manieră clară o reflecție profundă cu privire la modul în care ar trebui să arate schimbul de informații și sistemele informatice de mari dimensiuni la nivelul UE. Această reflecție ar trebui să țină seama în mod corespunzător de costurile pentru protecția vieții private și de eficiența aplicării legii, în primul rând atunci când sunt propuse și discutate noi instrumente, dar și după ce aceste instrumente sunt puse în aplicare, prin revizuirii periodice. Aceasta este o chestiune care necesită, de asemenea, garanții adaptate și o mai mare concentrare asupra principiului limitării scopului. Această viziune ar trebui să includă o reflecție asupra intrării (posibile) în vigoare a Tratatului de la Lisabona și a implicațiilor acestui fapt asupra sistemelor bazate pe un temei juridic cuprins în primul și în al treilea pilon.

*Evaluarea instrumentelor existente*

23. Prezentele propuneri au fost adoptate în plus față de instrumentele legale existente utilizate pentru consultarea amprentelor digitale, care nu au fost încă puse în aplicare pe deplin. AEPD evidențiază în acest context în special Decizia Prüm <sup>(16)</sup>, care trebuie pusă în aplicare de statele membre până în 2011. Pe baza acestei decizii, statele membre își acordă reciproc un acces automat, *inter alia*, la sistemele automate naționale de identificare a amprentelor digitale (AFIS) pe baza unei cereri de găsimă a unei concordanțe/lipse de concordanță. În cazul în care o căutare în temeiul Deciziei Prüm produce un rezultat pozitiv (o concordanță), se pot obține informații suplimentare, inclusiv date cu caracter personal, în statul membru care a înregistrat amprenta digitală în sistemul său AFIS național recurgând la legislația națională, inclusiv la asistență judiciară reciprocă.

<sup>(15)</sup> A se vedea nota de subsol 8.

<sup>(16)</sup> A se vedea, de asemenea, punctul 6 și nota de subsol 6.

24. Un alt instrument care ar putea fi util în acest context este Decizia-cadru 2006/960/JAI privind simplificarea schimbului de informații și date operative între autoritățile de aplicare a legii ale statelor membre ale Uniunii Europene<sup>(17)</sup>. Acest instrument facilitează schimbul de informații (de exemplu amprente digitale, precum și informații suplimentare) care sunt deținute de către autoritățile de aplicare a legii din statele membre sau care sunt puse la dispoziția acestora. Acest instrument este operațional din 18 decembrie 2008.
25. Singurul instrument care există mai demult și care este la dispoziția statelor membre este instrumentul tradițional de asistență judiciară reciprocă în baza căruia autoritățile judiciare ale statelor membre pot solicita accesul la colecții de amprente digitale de natură penală și nonpenală, inclusiv cu privire la solicitanții de azil în temeiul Convenției privind asistența reciprocă în materie penală.
26. AEPD consideră că este esențial ca în primul rând să se pună în aplicare și să se evalueze aplicarea noilor instrumente ale UE care permit consultarea de către un stat membru a amprentelor digitale și a altor date în materie de aplicare a legii deținute de un alt stat membru ca parte a evaluării necesității de accesare a Eurodac.
27. Respectarea principiului proporționalității presupune că măsura propusă este eficientă și, de asemenea, că scopul preconizat de propunere nu poate fi atins prin utilizarea instrumentelor existente. Respectivul instrumente trebuie evaluate cu atenție înaintea luării de măsuri suplimentare/noi pentru prelucrarea informațiilor cu caracter personal. Conform AEPD, o asemenea evaluare cuprinzătoare nu a avut loc.
30. Expunerea de motive a deciziei propuse afirmă că există un decalaj structural din punctul de vedere al informațiilor și al verificării, întrucât nu există în prezent un sistem unic care să fie accesibil autorităților de aplicare a legii și care să permită identificarea statului membru care deține informații cu privire la un solicitant de azil.
31. Aceasta poate fi situația, dar acest fapt nu răspunde la întrebarea de ce sunt necesare aceste informații privind solicitanții de azil care reprezintă, așa cum s-a menționat, un grup vulnerabil și, în principiu, nesuspectat, în condițiile în care nu sunt disponibile informații similare privind amprente digitale referitoare la orice alt grup din societate. S-ar putea ca motivele să fie întemeiate, dar nu sunt prezentate de către Comisie.
32. De asemenea, AEPD atrage atenția cu privire la o justificare ulterioară a propunerilor. Expunerea de motive din decizia propusă menționează că în cazul în care o căutare în temeiul Deciziei Prüm produce un rezultat pozitiv (o concordanță), se pot obține informații suplimentare, inclusiv date cu caracter personal, în statul membru care a înregistrat amprenta digitală în sistemul său AFIS național recurgând la legislația națională, inclusiv la asistența judiciară reciprocă. Acestea fiind spuse, Comisia pare să utilizeze ca argument în justificarea propunerii faptul că: „Deși ar putea fi încununată de succes în statele membre care stochează amprente digitale ale solicitanților de azil alături de alte amprente digitale colectate de autoritățile de aplicare a legii într-un sistem AFIS național, această procedură nu va da rezultate în statele membre care nu stochează amprente digitale ale solicitanților de azil în sistemele AFIS naționale decât dacă sunt legate de săvârșirea unei infracțiuni”. Acest argument este avansat și în evaluarea impactului care însoțește propunerile.

## VI. CIRCUMSTANȚELE SPECIFICE ALE CAZULUI PREZENT

28. Ca punct de plecare, AEPD ia notă de faptul că în comunicarea sa din 24 noiembrie 2005 Comisia a reamintit că: „Nici cererea de azil, nici cererea de viză nu indică în niciun fel că o persoană până la acel moment inocentă va comite o infracțiune sau un act terorist”<sup>(18)</sup>.
29. Propunerile se referă la accesul la datele cu caracter personal ale persoanelor fizice care nu numai că nu sunt, în principiu, suspectate de săvârșirea vreunei infracțiuni, dar care au nevoie, de asemenea, de un nivel mai ridicat de protecție din cauză că fug de persecuții. Aceste persoane reprezintă o populație deosebit de vulnerabilă, iar poziția precară a acestora trebuie luată în considerare în evaluarea necesității și a proporționalității acțiunii propuse.
33. În opinia AEPD un asemenea argument este lipsit de relevanță. Stocarea sistematică a amprentelor digitale ale solicitanților de azil care nu au legătură cu nicio infracțiune în aceeași bază de date cu alte amprente digitale colectate de autoritățile de aplicare a legii – ale solicitanților de azil și/sau ale altor persoane care sunt suspectate de a fi săvârșit infracțiuni sau care sunt condamnate – ridică serioase îngrijorări în ceea ce privește principiul limitării scopului și legitimitatea prelucrării datelor. În locul utilizării acestui argument, Comisia ar trebui să aprecieze dacă această stocare sistematică este în conformitate cu legislația UE în materie de protecția datelor.

## VII. CONTEXTUL PROPUNERII

34. Propunerile sunt adoptate de Comisie într-un moment în care contextul se află în schimbare.

<sup>(17)</sup> JO L 386, 29.12.2006, p. 89.

<sup>(18)</sup> Comunicare menționată la punctul 9 al acestui aviz.

35. În primul rând, adoptarea Programului de la Stockholm este prevăzută pentru decembrie 2009. În cursul acestor luni au loc discuții intense privind elaborarea acestui program multianual în domeniul libertății, securității și justiției. Schimbul de informații și utilizarea acestora vor constitui un aspect important al Programului de la Stockholm, inclusiv în ceea ce privește dezvoltarea unui model european de informare<sup>(19)</sup> sau a unei strategii europene de gestionare a informațiilor în domeniul securității<sup>(20)</sup>. În acest context, AEPD recomandă o abordare echilibrată, prin care garanțiile referitoare la protecția vieții private și a datelor să fie înscrise în sistemele de informații încă dintr-un stadiu incipient, pe cât posibil. În strânsă legătură cu Programul de la Stockholm se află, de asemenea, activitățile Grupului ad-hoc al Consiliului pentru schimbul de informații. Obiectul propunerilor respective va fi, cel mai probabil, acoperit prin intermediul acestor activități.
36. În al doilea rând, AEPD atrage atenția asupra necesității de a reflecta la consecințele pe care intrarea în vigoare a Tratatului de la Lisabona le va avea asupra viitoarei legislații privind activitățile de aplicare a legii. Prima consecință ar fi că orice propunere de acest fel va face, în viitor, obiectul unei proceduri legislative obișnuite, care presupune implicarea în egală măsură a Consiliului și a Parlamentului European. O a doua consecință este legată de eliminarea structurii pe piloni a Tratatului UE. Tratatul de la Lisabona ar putea necesita prezentarea de către Comisie a unei noi propuneri, care să se bazeze pe noul temei juridic și care, eventual, chiar să unifice regulamentul propus și decizia propusă într-un singur instrument juridic, ceea ce, în orice caz, ar contribui la claritatea juridică.
37. În al treilea rând, AEPD pune sub semnul întrebării, de asemenea, necesitatea adoptării acestei propuneri printr-o procedură distinctă de cea a reformării generale a regulamentelor Eurodac și Dublin, care se află încă în discuție în cadrul Parlamentului și al Consiliului. Consecința acestor propuneri este aceea că, în timp ce discuțiile fundamentale privind modificarea sistemului Eurodac nu au fost încă finalizate, scopul sistemului va fi schimbat, ceea ce reprezintă, de asemenea, o altă modificare fundamentală a sistemului. S-ar fi asigurat o mai bună consecvență dacă aceste propuneri ar fi fost unite în cadrul reformării generale<sup>(21)</sup> sau dacă ar fi fost amânate până după adoptarea primei modificări.
38. În aceste circumstanțe, este mai bine acum să se amâne adoptarea propunerii, în vederea evitării neclarității juridice. Comisia nu solicită ca propunerile să fie adoptate în regim de urgență, iar caracterul urgent nu este cu siguranță demonstrat nici de alte circumstanțe.

#### VIII. COMPATIBILITATEA CU ARTICOLUL 8 DIN CONVENȚIA EUROPEANĂ A DREPTURILOR OMULUI (ECHR)

39. Expunerea de motive a regulamentului propus se referă în mod explicit la respectarea drepturilor fundamentale, *inter alia* a articolului 8 din Carta drepturilor fundamentale a UE,

referitor la protecția datelor cu caracter personal. În expunerea de motive se arată că, în opinia Comisiei, pentru a asigura faptul că prelucrarea datelor cu caracter personal în scopul aplicării legii nu contravine dreptului fundamental al protecției datelor cu caracter personal, în special principiilor necesității și proporționalității, propunerea stabilește condiții stricte.

40. AEPD nu este convinsă de această declarație a Comisiei. AEPD afirmă că este crucial să se evalueze dacă propunerile fac dovada legitimității în temeiul articolului 8 din Convenția europeană a drepturilor omului, astfel cum a fost interpretat de Curtea de Justiție și de Curtea Europeană a Drepturilor Omului. Propunerile ar trebui să respecte principiile necesității și proporționalității, ținând seama de contextul instrumentelor care sunt deja disponibile. Comisia ar trebui să facă o demonstrație credibilă a acestui aspect în cadrul propunerii sau al expunerii de motive. Cauza care a stabilit un precedent în acest sens este *S. și Marper/Regatul Unit*<sup>(22)</sup>.
41. În considerentul (6) din decizia propusă se afirmă că „orice astfel de interferență trebuie să fie în conformitate cu legea, care trebuie formulată cu suficientă precizie pentru a permite indivizilor să-și adapteze comportamentul și trebuie să protejeze persoanele fizice împotriva arbitrarității și să indice cu suficientă claritate marja de libertate conferită autorităților competente și modul de exercitare a acesteia. Orice interferență trebuie să fie necesară într-o societate democratică pentru a realiza un interes legitim și proporțional și să fie proporțională cu obiectivul legitim pe care își propune să-l atingă”. Cu toate acestea, considerentele nu demonstrează de ce acest instrument propus este necesar.
42. Potrivit jurisprudenței consacrate a Curții Europene a Drepturilor Omului, o interferență este considerată necesară într-o societate democratică pentru un scop legitim, conform dispozițiilor articolului 8 alineatul (2) din ECHR, dacă răspunde unei „nevoi sociale presante” și, în special, dacă este proporțională cu scopul legitim urmărit și dacă motivele invocate de autoritățile naționale pentru a o justifica sunt „relevante și suficiente”<sup>(23)</sup>. Autoritățile naționale beneficiază, de asemenea, de o marjă de apreciere, „a cărei sferă de aplicare depinde nu numai de natura scopului legitim urmărit, dar și de caracterul specific al interferenței respective”<sup>(24)</sup>. Marja va tinde să se reducă în cazul în care dreptul respectiv este esențial pentru ca persoana să beneficieze efectiv de drepturile sale private sau fundamentale<sup>(25)</sup>.

<sup>(22)</sup> Cereri conexe 30562/04 și 30566/04, *S. și Marper/Regatul Unit*, hotărârea din 4 decembrie 2008, CEDO încă nepublicată.

<sup>(23)</sup> A se vedea, *inter alia*, hotărârea din 24 noiembrie 1986 în cauza *Gillow/Regatul Unit*, Seria A nr. 109, punctul 55.

<sup>(24)</sup> A se vedea hotărârea din 26 martie 1987 în cauza *Leander/Suedia*, Seria A nr. 116, punctul 59. A se vedea, de asemenea, hotărârea CJE din 20 mai 2003 în cauzele conexe C-465/2000, C-138/01 și C-139/01, *Österreichischer Rundfunk* și alții, Rec. 2003, p. I-4989, punctul 83.

<sup>(25)</sup> Hotărârea nr. 66746/01 din 27 mai 2004 în cauza *Connors/Regatul Unit*, punctul 82.

<sup>(19)</sup> Terminologie utilizată de Comisie în comunicarea sa din 10 iunie 2009, menționată în nota de subsol 8.

<sup>(20)</sup> Terminologie utilizată de Președinția suedeză.

<sup>(21)</sup> A se vedea punctul 4.

43. În acest context, este nevoie în primul rând să se evalueze scopul prelucrării planificate a datelor cu caracter personal: a fost scopul clar identificat? S-a dovedit că acesta respectă principiile necesității și proporționalității? Ar trebui să se dovedească, de asemenea, că nu sunt disponibile alte mijloace mai puțin invazive prin care să se atingă scopul prevăzut.
44. În propunere se afirmă că scopul sistemului Eurodac a fost modificat față de cel inițial, potrivit explicațiilor din considerentul (6) din decizia propusă<sup>(26)</sup>. Cu toate acestea, o simplă modificare a textului legislativ nu va avea drept rezultat o măsură care să fie compatibilă cu articolul 8 din ECHR. Se poate chiar argumenta că modificarea legislativă nu duce deloc la o schimbare a scopului. De asemenea, datele vor fi stocate și în viitor în sistemul Eurodac cu scopul unic de a facilita aplicarea Regulamentului Dublin. Numai în situații excepționale, astfel cum s-a arătat anterior în prezentul aviz, autoritățile de aplicare a legii din statele membre vor avea acces. Prin urmare, propunerile nu modifică scopul, ci trebuie să fie considerate drept excepții de la principiul limitării scopului, care poate fi permis în temeiul articolului 13 din Directiva 95/46/CE, în anumite condiții. Cu toate acestea, AEPD nu este convinsă că aceste condiții sunt îndeplinite în cazul de față.
45. AEPD subliniază în acest context faptul că simpla afirmare a unei modificări a scopului în cadrul unei propuneri legislative nu determină acceptarea acesteia. O modificare legislativă nu duce, în sine, la o evaluare diferită a necesității propunerilor într-o societate democratică, a proporționalității sau a acceptabilității acestora în temeiul dispozițiilor menționate la punctul anterior.
46. Caracterul intruziv al instrumentelor propuse de Comisie este evident. Cu toate acestea, utilitatea și necesitatea acestora sunt departe de a fi demonstrate în cadrul propunerilor. Necesitatea ar trebui dovedită prin demonstrarea cu dovezi substanțiale a legăturii dintre solicitanții de azil și terorism și/sau formele grave de criminalitate. Această demonstrație nu este realizată în cadrul propunerilor. Este adevărat că suspecții pot să fi intrat pe teritoriul UE prin introducerea unei cereri de azil false. Însă faptul că acesta este un scenariu posibil nu îl transformă într-un model general care să justifice adoptarea instrumentelor.
47. De asemenea, deosebit de îngrijorător în acest context este riscul de stigmatizare, rezultând din faptul că persoanele solicitante, care nu au fost condamnate pentru nicio infracțiune și care au dreptul la prezumția de nevinovăție, sunt tratate ca suspecți *a priori*<sup>(27)</sup>. În acest sens, Curtea Europeană a Drepturilor Omului are în vedere faptul că dreptul oricărei persoane, în temeiul convenției, de a fi

considerată nevinovată include regula generală potrivit căreia nicio suspiciune legată de nevinovăția unei persoane nu poate fi exprimată după ce aceasta este achitată<sup>(28)</sup>.

48. În plus, AEPD consideră că posibilul argument potrivit căruia accesul direct al autorităților de aplicare a legii la Eurodac este convenabil, ușor și rapid nu ar trebui să fie suficient pentru ca propunerea să facă dovada necesității. Demonstrarea necesității nu se poate baza numai pe utilitatea accesului, chiar și în contextul unor garanții stricte de protecție a datelor. Pe scurt, AEPD are îndoieli considerabile legate de legitimitatea propunerilor în temeiul articolului 8 din ECHR.

#### IX. CÂTEVA OBSERVAȚII REFERITOARE LA CONȚINUT

49. Numai printr-un „*obiter dictum*”, AEPD recomandă efectuarea unei precizări în textul articolului 2a din regulamentul propus sau, ca alternativă, adăugarea în decizia propusă a faptului că accesul la Eurodac poate fi acordat autorităților de aplicare a legii atunci când acestea au un motiv precis să considere că un suspect a mai solicitat azil. Acest aspect este sugerat în expunerea de motive, dar nu este inclus în textul propunerii propriu-zise. AEPD consideră că o astfel de garanție ar avea o valoare adăugată importantă. Însă această sugestie nu implică, în sine, acceptarea de către AEPD a principiului accesului autorităților de aplicare a legii la Eurodac. Trebuie înțeleasă ca o recomandare subsidiară.
50. AEPD constată, de asemenea, că accesul Eurodac la datele Eurodac nu este supus criteriilor stricte de acces la Eurodac impuse autorităților desemnate<sup>(29)</sup>. Cererile de comparare ale Eurodac sunt aprobate în scopul unei analize specifice sau al unei analize generale și de tip strategic. AEPD se întreabă cum ar putea facilitățile extinse ale Eurodac să corespundă argumentației oferite de Comisie, și anume că accesul este necesar numai pentru cazuri specifice, în circumstanțe specifice și în condiții stricte.

#### X. CONCLUZIE

51. AEPD are îndoieli serioase referitoare la legitimitatea propunerilor și la oportunitatea adoptării instrumentelor legislative pe baza acestor propuneri. Aceste îndoieli se bazează pe argumentele din prezentul aviz, care pot fi rezumate astfel:
52. AEPD dorește să evidențieze că un schimb de informații mai bun reprezintă un obiectiv politic esențial pentru Uniunea Europeană. Guvernele au nevoie de instrumente adecvate pentru a garanta securitatea cetățeanului, dar, în cadrul societății noastre europene, trebuie să respecte pe deplin drepturile fundamentale ale cetățeanului. Este sarcina legislatorului UE să asigure acest echilibru.

<sup>(26)</sup> A se vedea punctul 8 din prezentul aviz.

<sup>(27)</sup> S și Marper.

<sup>(28)</sup> Hotărârea nr. 28389/95 din 21 martie 2000 în cauza Asan Rushiti/Austria, punctul 31, cu trimiteri suplimentare, 33 CEDO 56.

<sup>(29)</sup> Articolul 7 din decizia propusă; a se vedea punctul 6 din prezentul aviz.

53. Măsurile de combatere a infracțiunilor cu caracter terorist și a altor infracțiuni grave pot reprezenta un motiv legitim pentru a permite prelucrarea datelor cu caracter personal, cu condiția ca necesitatea imixtiunii să fie sprijinită de elemente clare și indubitabile, iar proporționalitatea prelucrării să fie demonstrată. Acest lucru este cu atât mai necesar cu cât propunerile vizează un grup vulnerabil care are nevoie de o protecție sporită deoarece fuge de persecuții. Poziția precară a acestor persoane trebuie luată în considerare în evaluarea necesității și a proporționalității acțiunii propuse. AEPD subliniază, de asemenea, riscul stigmatizării.
54. AEPD recomandă evaluarea legitimității propunerilor într-un context mai larg, în special:
- (a) tendința de a acorda autorităților de aplicare a legii accesul la datele cu caracter personal ale persoanelor fizice care nu sunt suspectate de săvârșirea niciunei infracțiuni și care au fost colectate în alte scopuri;
  - (b) necesitatea unei evaluări de la caz la caz a fiecărei propuneri de acest fel și a unei viziuni coerente, cuprinzătoare și orientate către viitor, de preferință din perspectiva Programului de la Stockholm;
  - (c) necesitatea ca în primul rând să se pună în aplicare și să se evalueze aplicarea altor noi instrumente ale UE care permit consultarea de către un stat membru a amprentelor digitale și a altor date în materie de aplicare a legii deținute de un alt stat membru;
- (d) caracterul urgent al propunerii, având în vedere climatul juridic și politic în schimbare.
55. În ceea ce privește compatibilitatea propunerilor cu articolul 8 din ECHR, AEPD pune sub semnul întrebării modificarea scopului sistemului și subliniază faptul că simpla afirmare a unei modificări a scopului în cadrul unei propuneri legislative nu reprezintă modificarea în sine. În plus, o modificare legislativă nu duce, în sine, la o evaluare diferită a necesității propunerilor într-o societate democratică, a proporționalității sau a acceptabilității acestora, în special din perspectiva normelor privind limitarea scopului din Directiva 95/46/CE.
56. AEPD subliniază faptul că necesitatea ar trebui dovedită prin demonstrarea cu dovezi substanțiale a legăturii dintre solicitanții de azil și terorism și/sau formele grave de criminalitate. Această demonstrație nu este realizată în cadrul propunerilor.
57. În cele din urmă, AEPD salută faptul că este consultată și recomandă ca trimiterea la această consultare să fie făcută în considerentele propunerii, în același fel în care a fost făcută într-o serie de alte texte legislative cu privire la care AEPD a fost consultată, în conformitate cu Regulamentul (CE) nr. 45/2001. De asemenea, AEPD face câteva observații referitoare la partea dispozitivă a propunerilor.

Adoptat la Bruxelles, 7 octombrie 2009.

Peter HUSTINX

*Autoritatea Europeană pentru Protecția Datelor*